

BTEC NATIONAL IN IT

Learner Companion

Unit 1: Information Technology Systems

zigzageducation.co.uk

POD
11526

Publish your own work... Write to a brief...
Register at publishmenow.co.uk

Follow us on Twitter @ZigZagComputing

Contents

Product Support from ZigZag Education	ii
Terms and Conditions of Use	iii
Teacher's Introduction.....	1
1. A: Digital devices in IT systems.....	2
A1 Digital devices, their functions and uses	2
A2 Peripheral devices and media	8
A3 Computer software in an IT system	13
A4 Emerging technologies	23
A5 Choosing IT systems	27
2. B: Transmitting data	30
B1 Connectivity.....	30
B2 Networks	37
B3 Issues relating to transmission of data.....	41
3. C: Operating online.....	46
C1 Online systems	46
C2 Online communities	54
4. D: Protecting data and information.....	63
D1 Threats to data, information and systems	63
D2 Protecting data.....	70
5. E: Impact of IT systems	80
E1 Online services.....	80
E2 Impact on organisations	87
E3 Using and manipulating data	92
6. F: Issues	101
F1 Moral and ethical issues	101
F2 Legal issues	109
Answers	116
Learning Aim 1.....	116
Learning Aim 2.....	118
Learning Aim 3.....	119
Learning Aim 4.....	120
Learning Aim 5.....	121
Learning Aim 6.....	122

Teacher's Introduction

This companion has been written specifically for the Level 3 BTEC IT qualification (first teaching from September 2016). The theory notes and practice questions cover the essential knowledge and understanding prescribed in the BTEC Unit 1 specification.

About Unit 1: Information Technology Systems

Unit 1 (120 GLH) is assessed using a 2-hour (90-mark) written examination, which is set and marked by Pearson. There are two opportunities for assessment each year – in January and in June.

Unit 1 is a mandatory unit in the *Extended Certificate* (360 GLH), *Foundation Diploma* (510 GLH), *Diploma* (720 GLH) and *Extended Diploma* (1080 GLH).

Each of the six *Learning Aims* (1–6) is given its own section in the resource. These are as follows:

- ① *A: Digital devices in IT systems*
- ② *B: Transmitting data*
- ③ *C: Operating online*
- ④ *D: Protecting data and information*
- ⑤ *E: Impact of IT systems*
- ⑥ *F: Issues*

Remember!

Always check the exam board website for new information, including changes to the specification and sample assessment material.

Within each section there are student notes covering the specification content and structure. These notes include descriptions of theory, supported with examples, diagrams and images where appropriate.

Questions are interspersed throughout the guide to test and develop understanding. Suggested answers are included at the back of the resource.

NB The intention of the suggested answers is to save the teacher time, rather than to offer a comprehensive set of definite answers. In some cases, there are equally valid alternative answers to those that have been given.

March 2022



A web page containing all the links listed in this resource is conveniently provided on ZigZag Education's website at zzed.uk/11526

You may find this helpful for accessing the websites rather than typing in each URL.

① A: Digital devices in IT systems

In this chapter you will learn:

- ① Types of digital devices, their functions and uses
- ① Types of peripherals and accessibility devices
- ① The types, uses and roles of operating systems
- ① The types, uses and roles of utility and application software
- ① The uses of emerging technologies
- ① The factors in choosing an IT system

A1 Digital devices, their functions and uses

An IT system is a group of interconnected devices which run different software, e.g. Think about the devices in your home or school that are connected to the network. TVs, games consoles, etc. Each has a very different use, ranging from work, leisure, some have more than one function – you can use a laptop to do your schoolwork or a video call. Some are fixed with permanently wired power and Ethernet; others are handheld, run on batteries and are wirelessly networked.

Digital devices

Below is a selection of the devices that make up IT systems.

Multifunction devices

A **multifunction device** has different functions (capabilities) built in. Good examples include a mobile phone (which can serve as a satnav, a camera, a web-browsing device etc.), and a printer with a flatbed scanner, such as the one shown in the picture.

This is a very basic device which can be connected to a PC to print and scan. It can be used without a PC, as a photocopier. You might also be able to insert a flash card or USB thumb drive to print documents and photos directly from the printer. In the past, you typically had a separate scanner and printer – two large devices whereby you would scan on one and print from the other. The beauty of the multifunction device is that it is space-saving, time-saving and easy to use. However, if one part breaks, such as the scanner, the whole device may need to be replaced.

If you take a look online, you'll find all sorts of weird and wonderful multifunction devices, such as a fridge with a built-in coffeemaker, or a more practical light with a built-in fan.

A laptop or tablet is really a multifunction device as well because it is so versatile.

Personal computers

The 'PC' as we know it was first introduced in 1981 – that's just over 40 years ago! IBM took a bunch of off-the-shelf components and wrote a special BIOS, and combined it with an operating system called DOS. Competing manufacturers tried to emulate the IBM machine as closely as possible so that the same software could run on their 'clone' machines (and yes, there were lawsuits involved over the recreation or parody).

**COPYRIGHT
PROTECTED**



Over the years, vastly more powerful machines have been developed, and these systems and application programs.

PCs are still the workhorses of offices, and are used in many homes. Nowadays, the desktop PC – have made inroads into the PC market for their flexibility. Their and having small hard disks has been dispelled, and the prices have dramatically

Laptop: a portable computer with a (touch)screen, touchpad and keyboard and IO Thunderbolt ports. Provides much of the functionality of a desktop computer but Wi-Fi built in as standard. Often used in homes and businesses.

Desktop computer: the traditional computer. Powerful processing and high-performance base unit and peripherals such as a keyboard, mouse and large screen. Some are screen. They must be connected to power and usually are connected to resources (printers and files) using a network cable.

Mobile devices

Below are some examples of portable and wearable devices.

Mobile
commu
mobile p

Smartphone: a mobile telephone with a relatively small screen running an operating system like iOS. The user typically uses a touchscreen and an onscreen keyboard, rather than a physical keyboard. Smartphones are used for calls, texts, emails and other communications. Social media apps connect to the Internet over Wi-Fi and mobile data network.

Small tablet: a thin, portable device that is larger than a smartphone – usually with cellular access. Small tablets are used for light web browsing and email, gaming and not using desktop applications.

Large tablet: larger and more powerful hardware than a smaller tablet, making it suitable for different circumstances.

Smartwatch: used as a timepiece (similar to a traditional watch that is worn on the wrist) and can connect to a phone to display messages and notifications. May have a fitness tracker built in.

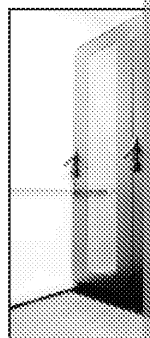
Fitness tracker: measures heart rate, number of steps taken, etc. Can be a stand-alone device or part of a smartwatch.

Servers

Servers are very powerful computers with lots of RAM (memory), fast processors and lots of disk space (normally lots of separate disks joined together, called a redundant array of independent disks, or 'RAID', where if one disk fails the server carries on working). They 'serve up' information to the 'client' computers – the computers on the desks in organisations. They often run special operating systems such as Windows Server, or a distribution of Linux. They need to run 24/7/365 with minimal downtime. Sometimes, several servers can be installed on a host machine, each with a different purpose. Or separate physical servers are used.

Servers are kept inside special secure rooms within a business, usually mounted in racks or cabinets. Some servers are located in Internet-connected data centres which host web pages and file storage in the cloud. When you first set up a server, you need to configure the server with specific roles.

Server
network
Facilitate
serves w



**COPYRIGHT
PROTECTED**



A large organisation will usually run several servers, each for a different purpose. So

- Domain controller that manages usernames and passwords, client PCs, and the large network)
- Dedicated file server – stores users' personal files and shared drives
- Print server – manages shared printers
- Web server – hosts web pages and provides them to the client's web browser. It also include a DNS server, which converts a web address into the IP address of the server. The server caches the web pages from the public Internet that have been requested. This speeds up the page load times as the page is stored locally.
- Email server – stores and distributes email

If you decide to work in IT, you'll be working with servers and PCs!

Entertainment systems



There are various types of **entertainment system**. Perhaps one of the most obvious examples is a PC or laptop that you use to stream video from either YouTube or a service such as Netflix, or music from Spotify. Sometimes a computer is used within a home cinema system.

Specific entertainment systems include:

Smart TVs: televisions with extra services – such as streaming apps and web access (usually built in).

Games consoles: produced by companies such as Sony, Microsoft and Nintendo, may also be used for streaming TV, films, music and web access to a television set. They are also used as desktop PCs (but usually with a more attractive case design). Some consoles still allow playback of DVDs, Blu-ray disks and CDs. A games console is usually controlled by a game pad.

Smart speakers: although Amazon's Echo, Google's 'Home' range and Apple's HomePod are used for entertainment purposes, such as controlling other home devices or using the web, their most frequent use is probably as music players.

Still and video cameras

Consumer digital cameras have been around since the mid 1990s and have replaced film cameras for all but a few film enthusiasts. Most modern cameras can record both still and moving images.

Most people will use the digital camera built into their smartphones for most day-to-day photography. Smartphones are great for recording short video clips. The cameras in smartphones have vastly improved in recent years in terms of quality (megapixels) and features, and many will shoot 1080p HD video.

Simple point-and-shoot digital cameras can record still and moving images, usually to a memory card. The images are retrieved by plugging the memory card or camera into the PC, or across a wireless network.

Professionals and photography enthusiasts will use more expensive digital single lens reflex (DSLR) cameras for the increased quality, optical zoom and high video quality.

**COPYRIGHT
PROTECTED**



Specialised video cameras are available for shooting in ultra HD (4K and 8K), which can take 10,000 frames per second. You can see some impressive slow-motion shots of lightning and glass breaking. Most TV programmes and feature-length films are now shot in 4K.

If you've ever watched the film *Steve Jobs*, released in 2015 (age rated 15), you may have noticed that the image quality changes throughout the film. This is because the film was filmed using 16mm film for the early scenes and digital for the later scenes. You can really notice the increase in sharpness of the scenes that were shot digitally. The film's part set in 1998 contrasted with the graininess of the early scenes shot on 16mm film (which was an acceptable quality for a feature-length film).

We also have 'webcams' built into our laptops and tablets, and front-facing cameras on smartphones. These can be used to make video calls (and maybe take the odd selfie...). Other examples of video cameras include security cameras, dashcams and helmet cams.

Navigation systems

A **navigation system** pinpoints your location on a map, often using the global positioning system (GPS) that calculates our location – sometimes to within a few centimetres – using a network of 31 satellites. It uses this information to calculate a route for us to take – to drive in a car, to cycle, or even to pilot a ship. We enter an intended destination, and the device works out the best route and an estimated arrival time (or at least it should...). The device, mounted at the corner of the windscreen or built into the dashboard, reads out driving instructions, and can be quickly glanced at when driving.

A satnav is either a stand-alone device that has a built-in map, or the device itself is built into the console of a car's dashboard. Many smartphones also use a GPS built in, but the maps app on phones usually downloads the base map in real time using the cellular network, and can show traffic updates and even change the route if there is an accident or a hold-up.

Walkers, outdoor enthusiasts and geocachers often use stand-alone GPS receivers. However, a phone's GPS signal can be patchy in remote areas.

Navigation systems have revolutionised the way we travel – no more time wasted waiting for driving instructions – but we are quickly losing the map skills that could keep us on our way if a phone signal is lost.

Navigation systems are becoming more common as journeys are becoming longer and more complex. In the future, self-driving vehicles, in traffic, will be able to navigate themselves.



Navigation systems are also used in shipping – ships are guided by GPS into dock. In the future, we could have self-driving boats. For a look at <https://www.rivieramm.com/content-hub/futuristic-passenger-ships-navigation-revealed-55725>



Data capture and communication systems

There are many different types of equipment that use sensors or input devices to collect data and store the data for later retrieval, or data transmission in real time. The systems could be as commonplace as a barcode or QR code reader in sales or stock control systems, or an ordering system, or specialist devices that measure earth tremors or the height of a building.

Data capture systems are used to collect information that it can later be used for. It can be as simple as a barcode reader.

Communications devices and systems

Communications devices include all manner of telephone handsets and the networks that connect them. They also underpins computer systems, the Internet and telephone networks.

**COPYRIGHT
PROTECTED**



The functions of digital devices

The devices we've just talked about, and others, can be used in a wide variety of

Education and training

Anyone at school or university in 2020–2021 will have first-hand experience of education and training – that will include you! Here are just a few of the uses of

- Use of smartboards and data projectors and tablets in the classroom
- Electronic resources, Internet research, online learning platforms and video
- Upload and download of files to a VLE (virtual learning environment), including coursework submission
- Video courses/tutorials
- Taking exams online

Personal

Ask yourself – what equipment, resources and apps do you use in your free time? Mobile phone? Laptop? Do you surf the net, chat with friends, stream video, or play games online?

Social

Again, you probably use smartphones, tablets and laptops fitted with cameras and access friends online, and maybe even the webcams built into some TVs and games consoles. You use these devices to access social media, upload photos and set your status.

Retail

A lot of technology is used in retail – you'll see some of it as a customer, and the examples include:

- Online websites and sales platforms (using web servers, network infrastructure and personal devices)
- Stock control systems that monitor stock levels and order more from the warehouse tracked using barcodes and handheld scanners, or RFID tags (that are faster)
- Checkout equipment – tills or self-service checkouts – uses barcode readers and receipt printers
- Electronic payment systems used to make card transactions with your bank
- Database systems that record all transactional data

Organisations

Organisations use a wide variety of equipment to build up their IT system and networks. Laptops, mobile devices, printers, scanners and servers are almost guaranteed. So are systems for internal communications between the staff, and external to allow communication with customers and other businesses. For example, a management information system (MIS) used by a school allows teachers (internal staff) to access their students' assessment grades over a period of time. They can use it to look for patterns of which students are struggling and need improving. The same system could be used by parents (external stakeholders) to access their child's grades or homework information.

Many organisations use modern equipment, but may be keeping alive systems that are old but aren't broken. If a system still provides the required functions, then don't fix it. A 20-year-old system may be perfectly functional, or an old finance system dating back 40 years may still be as useful as when it was first virtualised. A lot of companies are now reaping the benefits of using the cloud for managing applications, although on-premises servers are still popular.

**COPYRIGHT
PROTECTED**



Creative tasks

Creative tasks could include editing photos, graphic design, animating film clips or developing games. Designers use a wide range of cameras and scanning equipment and storage. Companies that edit video will have fast networks and servers. Applications run expensive software suites from Adobe and other companies, although PC versions

Questions – A1 Digital devices, their functions and uses

1. Why is a laptop really a multifunction device?
2. Give an example of one type of entertainment system in your home, and use it for.
3. Why might navigation apps installed on a smartphone provide a better experience than a specialised satnav device?
4. Suggest two ways that technology has changed retail.
5. Give an example of a device that is usually only used within businesses, rather than in the home.

INSPECTION COPY

COPYRIGHT
PROTECTED



A2 Peripheral devices and media

Devices attached to a computer are often called peripherals. They are often plugged into specialist 'ports' for displays and older legacy connections. Take a look at the ports alongside USB, you might see USB C, HDMI, a 3.5 mm headphone socket and Ethernet input and output, or increase the storage space available to the system.

Peripheral devices

Input devices

Input devices are used to send data to the device.

For example:

- Keyboards are used to enter data into a system which is then processed in order for a letter, number or symbol to appear on a screen.
- Mice, trackballs, trackpads and other pointing devices such as digital pens and styluses are used for screen navigation and clicks.
- A document scanner or flatbed scanner digitises paper records and images.
- A barcode scanner or camera reads barcodes and QR codes.
- A webcam for video calling.
- A microphone for voice control or input.

Output devices

Output devices provide visual, printed or audio output.

For example:

- The screen (display) to show output from the operating system, applications and media such as images and video. Some users connect a second display.
- Speakers or headphones/earbuds to provide audio from the operating system.
- A printer to produce 'hard copy' output on paper.
- A 3D printer to 'print' objects. Most would use plastic filament, but some can use metal.

Remember that some peripheral devices are **both input and output devices**.

For example:

- A multifunction printer provides output (printed documents) and accepts input from the scanner.
- A smart speaker provides audio output but also uses a microphone to allow voice control input.
- A touchscreen outputs the video display but also provides input from your taps and swipes.
- A games controller accepts input from the buttons but provides tactile feedback such as vibration, as output.
- A headset provides audio output from the speakers and voice input from the microphone.

**COPYRIGHT
PROTECTED**



Storage devices

We'll cover the actual storage media in a moment, but here's a quick rundown of the actual **storage devices** used in conjunction with the media:

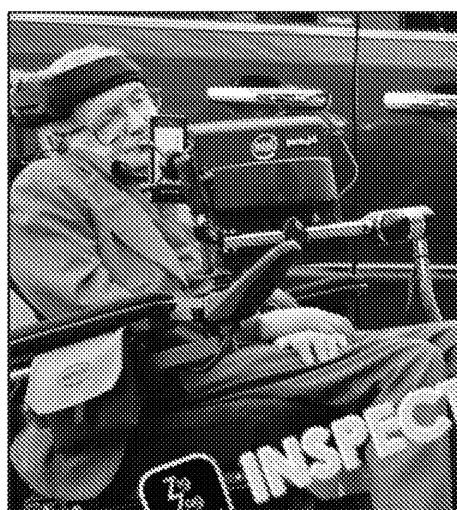
- As well as internal hard drives, you can get external hard drives. Many hard drives can be purchased as external units that plug in via USB – great for large file transfers, storage and backups. Docks (sometimes called plug in internal drives to temporarily copy data to and from drives, and to for
- Card readers – allow a variety of flash storage cards to be accessed over USB of card, such as SD cards and CompactFlash used in digital cameras.
- USB flash drives (aka thumb drives or pen drives) contain flash memory chips
- DVD drives – most modern consumer-grade PCs and laptops no longer feature external USB drives are readily available.
- Floppy drives – yes, you can still buy external USB floppy drives – great if you from 30 years ago! Just don't expect the disks to be 100 % reliable and free able to find an application that can properly open the files.

Manual and automatic data processing

Manual data processing is where data is typed into a system and processed by the user; for example, you could type data into a spreadsheet and create a graph, manually adding and configuring the title and axes labels.

With **automatic data processing**, you would still manually input the data, but the data is automatically processed so a chart or report is automatically generated. Another example would be the sale of a software download. The customer would manually select the product and enter their payment and contact details into their website. The system could then automatically generate and send an email that contains a download link and product key, with a VAT receipt attached as a PDF.

Accessibility devices



Many different **accessibility devices** are available to allow people with disabilities or medical conditions to successfully operate a computer.

Why not take a look at the equipment that Stephen Hawking used in

Some of the most basic controls can be tracking for people with limited mobility. They often come with settings that allow graphics and magnification or adjustable

For people who find typing or using a normal keyboards, sideways mice and trackballs

More specialist equipment includes specialist keyboards with different buttons, feet, or a sip-and-puff device that allows control by the mouth. Optical character a blind or partially sighted user to have paper documents read aloud.

**COPYRIGHT
PROTECTED**



Storage media within an IT system

Below are the common types of **storage media** that are still in use.

Each has a specific purpose and must be specifically chosen for the environment it will be used for. For example, a solid-state drive wouldn't be used for archiving if it is too small and expensive. A mechanical drive might be used instead. But you wouldn't use a mechanical drive in a rugged environment where it is likely to be dropped because it is not as durable as a solid-state drive.

Magnetic storage

Magnetic storage uses a metallic oxide media such as iron, which may be 'doped' with cobalt. A magnetic write head aligns crystals of the oxide coating depending on the data being written. A read head can then read back the recorded data.

There are two modern uses of magnetic storage:

1. **Mechanical hard drives** – use aluminium (or sometimes glass or ceramic) disks coated with the oxide. The read-write head hovers just above (but doesn't touch) the surface. Cheaper consumer computers still use mechanical drives because they are cheaper than solid-state drives, and many servers still use large mechanical drives for their cheapness and large capacity (they spin much faster than the ones in desktops are larger (3.5") while laptop versions are smaller (2.5"). You can find them e.g. housed in a plastic case and plugged in by USB. They are available in various terabytes of storage.
2. **Tape** – computers used to use reels of plastic tape coated with the oxide for everyday storage. But now the tape is housed inside cartridges, and only used for backups. Although hard drive and cloud-based backups have reduced the need for tape, tape is still used and new tapes are still being developed, offering greater capacity and faster speeds in the same small cartridges. Unlike disks, the heads actually touch the tape, so the heads occasionally require cleaning to remove a build-up of oxide particles.
3. There are other forms of magnetic media available, such as floppy disks with a save icon for most software packages if you've never seen one) and larger ZIF disks today, apart from in legacy systems.

Optical storage

These include the shiny silver plastic disks such as CDs (compact disks), DVDs (digital versatile disks) and Blu-ray (BD). Each was released at a different time, for a different purpose.

The disks are read by a laser – hence the name 'optical'. Their use has rapidly declined in recent years (replaced with digital downloads and streaming), and most consumer computers and laptops no longer have an optical drive fitted as standard.

Most commercially produced disks are printed at a factory and are called ROMs (Read Only Memory). Their contents cannot be modified.

Home users can purchase writable (and rewritable) media such as CR-R and DVD-R. There are different ways that the data can be written to by the laser for DVDs, but most drive types of disk). These disks are typically less durable than factory-printed versions.

**COPYRIGHT
PROTECTED**



Each type has a different capacity:

- CD – up to 700 MB or 80 minutes audio
- DVD (single layer) – 4.7 GB / (dual layer) – 8.5 GB (often called DVD 9)
- Blu-ray (single layer) – 25 GB / (dual layer) – 50 GB

A DVD drive can typically read CDs, and a Blu-ray drive can typically read DVDs and only read CDs, and a DVD drive cannot read Blu-ray.

Each type also has different uses:

- **Commercial PC software and games** were once sold mostly on **CDs** (and later became larger and DVD drives became common), but now they are mostly sold as digital downloads from a 'digital store' set up by the manufacturer.
- **Computer games for consoles** can still be purchased on disk (used to be **CDs** or **Blu-ray**) in addition to digital downloads from a 'digital store' set up by the manufacturer.
- **Music** was typically sold on **CD** since the 1990s (when CDs replaced vinyl and music is streamed or downloaded).
- **Films and TV shows** were typically sold on **DVD** starting in the late 1990s (the 2000s), and later **Blu-ray** for high-definition versions.

Over the years, individuals have sometimes used optical media to perform backup of their data, but this has largely been replaced with hard disk or cloud-based alternatives.

Solid-state storage

High-end modern devices, and many portable devices, use **flash memory** – there are no moving parts, hence 'solid state'. This memory retains the data when switched off (non-volatile) and can be used in place of a mechanical drive.

There are many modern uses of flash memory:

1. Hard drives – a much faster replacement for mechanical drives
2. Storage in portable devices (phones and tablets), and devices such as the Raspberry Pi – either built-in or using a removable card (e.g. SD or micro SD)
3. Storage in cameras and other monitoring equipment (e.g. SD and other similar cards)
4. USB flash drives (pen drives or thumb drives) – used for data transfer or sharing between devices

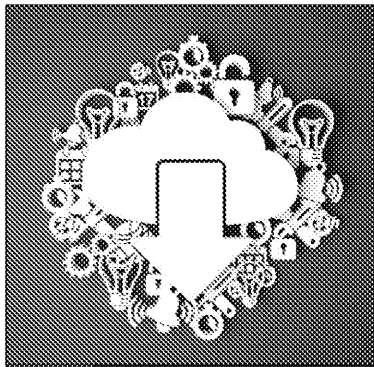
As you can see, there are lots of potential uses for these types of storage in everyday life:

- Using mechanical or solid-state hard drives as the main primary storage in your computer
- Backing up data to tape or cloud (businesses) or to an external drive (household)
- Using an external drive to store large files such as many years' worth of digital photos
- Sharing files with your family using the cloud
- Saving your schoolwork on the cloud, or transferring your schoolwork home
- Using an SD card or a MicroSD card in your camera or smartphone
- Watching a film on a DVD or Blu-ray disc

**COPYRIGHT
PROTECTED**



Cloud storage



Cloud storage is data that is stored on a server somewhere else and is available to access via the Internet. Server farms, also called data centres, are owned by large companies such as Google and Microsoft.

You need to create an account and set up a user to store the data. Providers usually give each user a small amount of space, typically 2–15 GB – but if you want more space you can pay an annual fee which you can change as needed. You can access the data in a web browser or 'synced' through an app. Anything that you add to that folder gets uploaded to the cloud and anything deleted from the cloud is downloaded from the cloud.

Cloud storage is great for:

- Backups (e.g. personal use includes your phone automatically backing up photos to Apple's iCloud).
- Sharing files with friends and family (e.g. sending files using Dropbox).
- Businesses don't have to rely on onsite servers, making their files more accessible (e.g. Amazon Web Services).
- Working offline with automatic syncing when you reconnect (e.g. a feature called 'offline mode' with OneDrive storage).

Questions – A2 Peripheral devices and media

1. Give an example of a device that functions as both an input device and an output device and explain why it falls into both categories.
2. Explain why automatic data processing is cost-effective.
3. Give two examples of an accessibility device that would be useful to someone who is partially sighted.
4. Explain one type of media that would be suitable for a backup media.
5. Explain why solid-state storage has benefits over magnetic media.

INSPECTION COPY

COPYRIGHT
PROTECTED



A3 Computer software in an IT system

When you first turn on a computer or a laptop, the first thing that runs is either a low-level software that resides in a chip on the motherboard, wakes up the hardware and the operating system. A BIOS is found on older computers, whereas an UEFI on more sophisticated, supports graphics and mice, and includes security features.

Types of operating system (OS)

Today the most common **operating system** on desktop/laptop computers by far is Windows (currently Windows 11), followed by macOS. There's no doubt that you'll be familiar with using either or both of these. By the time you read this, Windows 12 will have been launched.

Linux is a free alternative and has a cult following with computer enthusiasts. While its (distributions) are geared to be accessible to consumers with a GUI, it has a reputation with more frequent use in the terminal. If you're interesting in trying out Linux, you should first try installing a popular distro such as Mint or Ubuntu either as a virtual machine or as a live boot (a live boot doesn't install to your hard drive) – both can be booted in a virtual machine manager such as VirtualBox. If you've got a Raspberry Pi, you'll probably be using a version of Linux.

On the phone and tablet side, Android (from Google) and iOS/iPadOS (Apple) are the two dominant players. Interestingly, Apple uses a dedicated OS for its various types of device, such as iPadOS for tablets and tvOS for Apple TV.

There is significant overlap in the design and core feature sets between competing platforms, and over the years there have been lawsuits over these similarities. If you are familiar with using one, you will pick up the other fairly quickly.

A key difference between these systems is the types of software. Software is typically written for a specific operating system and is then ported over to another. Some software or apps may only be written for one system, especially if the software is written by either Apple or Microsoft, or by a very small developer.

Real-time

Real-time operating systems constantly input, process and output information instantaneously, otherwise the system will fail. Examples include airline control and ticketing systems, as well as the control systems for the aircraft itself.

Single-user single task

One user can only run one application at a time. These are often used in embedded systems that perform only one function, and simple devices such as non-smartphones. Older computers running command-line operating systems such as DOS (disk operating system) could only run one application at a time, and it was difficult to copy and paste information between different applications.

Single-user multitasking

Windows is a good example of this type of OS – only one user can be logged in at a time, but lots of different applications can be run simultaneously. Windows was named for this reason – applications could run in separate 'windows' and you could switch

**COPYRIGHT
PROTECTED**



copy information between each window. The earliest versions of Windows were just off the command line, DOS, rather than being fully fledged operating systems (unlike you use a tablet to both play music and search the web at the same time, your device

Multi-user

As the name suggests, more than one user can use the computer at the same time. Servers and mainframe computers run such operating systems, with each user sharing the processor and system resources. By default, two users can simultaneously connect to a Windows server through remote desktop in order to use the graphical desktop environment (covered later), but more users can be allowed to use the server if additional licences are purchased.

The role of the operating system

The operating system is one of the most important parts of a computer – it interfaces the hardware, the user, the application software, and provides the environment for the application software to run in.

Networking

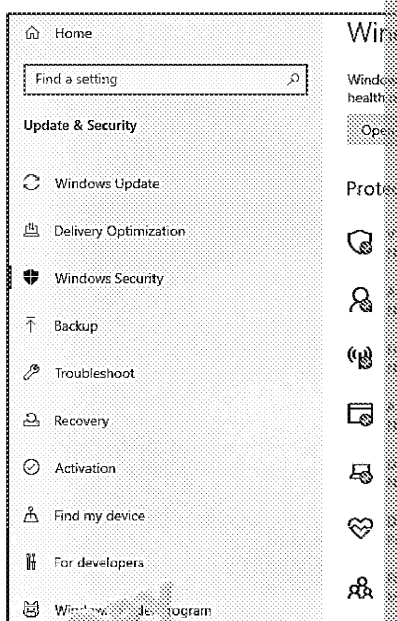
The operating system is responsible for negotiating and managing connections from networked devices and the Internet. The OS also allows applications to access the network. When you connect to a network, you may need to provide certain details, which are remembered by the OS. These can be usernames and passwords, or network settings (speed or duplexing) if these cannot be remembered. If the network has no security, only the network name (SSID) will need to be selected.

Security

Our devices contain lots of data that hackers want to steal, and are targets for malware (see Section D). Therefore, it is essential that they are protected.

Most operating systems include a firewall (usually incoming) to block intrusions. Some also have built-in antivirus software, such as Windows Defender Antivirus. Both firewalls and antivirus are covered in a later section.

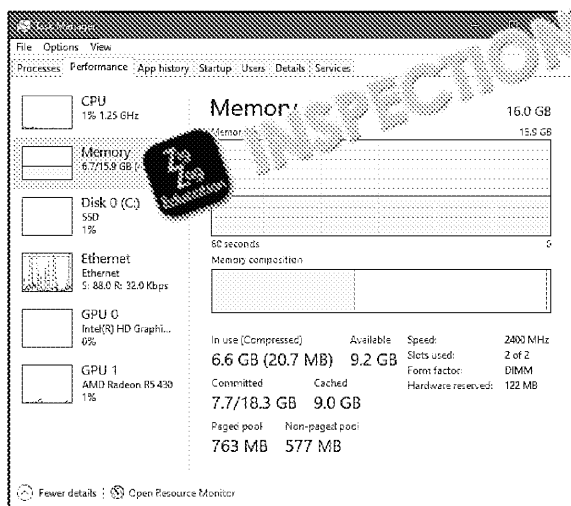
The operating system is also capable of managing the permissions of files and drives – the network administrator will be able to allow or deny access to certain files or folders to different users, and decide whether users can edit and delete files, or just view their contents.



Memory management

Operating systems manage the memory (RAM). When the RAM becomes full, the system can 'borrow' memory from the hard drive using a 'swap file', and the memory controller manages the RAM and hard drive using a 'swap file'. The swap file is slower than RAM because of the mechanical nature of the hard drive, especially if slower mechanical system to run slowly.

In Windows, you can use the 'Performance' app to see how much RAM is currently in use.



COPYRIGHT
PROTECTED



Multitasking

Multitasking is an interesting concept. The processor is shared between each running application. Each application gets a short amount of processing time before the next application gets a turn. This switching happens so quickly that all of the applications appear to run at once.

In the old days, if one application crashed, the whole system would lock up, and you had to reboot the system. This is because computers used 'cooperative multitasking' – each application releasing its control of the processor – if that program crashed, it couldn't release its control. Modern operating systems use 'pre-emptive multitasking' – each program is given a set processor time and if a program crashes, all other programs keep running.

Interrupts are sent to the processor from hardware or software either when a process needs to be displayed. Interrupts occur each time you press a key on the keyboard or receive a message from the network. The OS knows when a key has been pressed or a message has been received.

Device drivers

All peripheral devices, keyboard, mouse, game controller, printer, scanner, webcam, speakers, displays, external drives, are managed by the operating system; for example, the recording and storing of input and providing it to the appropriate program, or sending the necessary output to the monitor, printer, etc.

Each device uses a special piece of software called a **driver** to allow it to communicate with the OS (to send and receive data). Some drivers are built into the OS, while others are provided by a third party, such as a printer manufacturer. Often drivers are written for one or a few specific devices. You will find different drivers for the 32 and 64 bit versions. You will find different drivers for different Linux distros.

The operating system will usually have drivers for basic devices such as keyboard and mouse. To add devices newer than the OS, or to unlock all of the features, specific drivers may be required. For example is a printer. Sometimes when you connect a printer to Windows, the OS will download the Windows Update if one is available there. When you send a file from a word processor to a printer, the driver converts the documents into a format that the printer can understand.

Operating system user interfaces

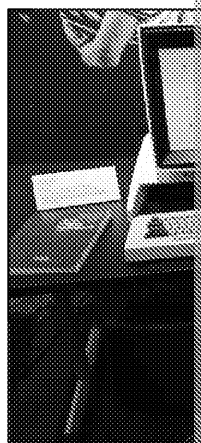
Computers and devices provide very different user interfaces depending on their hardware and software base. The user interface is what is shown on the screen for us to interact with.

Graphical user interface (GUI)

The GUI is what we mainly use today on PCs and laptops. Both Windows and macOS have been GUI-based since they were first developed in the 1980s. However, early versions of Windows required you to boot into the command line called DOS before you could open a graphical shell.

The photograph shows the Xerox Alto computer, one of the first GUIs developed in the early 1970s.

We are all familiar with the desktop metaphor – the early designers of the GUI looked around their offices and decided to digitise what they saw. What's in an office? Well, your desk, so you can put paper on and work on paper – so we got the desktop where you could store files and see open applications such as word processors. Then there's a waste paper bin – so we got the trash can, so we got a file explorer... etc. Some early desktops even had inboxes where you would receive and send mail!



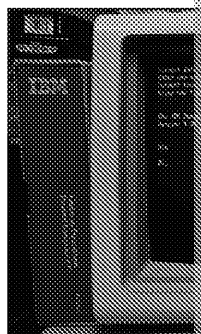
**COPYRIGHT
PROTECTED**



GUIs are designed to be navigated using a keyboard and mouse (although modern touchscreens as well). They employ an interface called WIMP – windows, icons, menus, and pointers – which is much more intuitive and friendly compared to the CLI (see below) because you click and press buttons rather than typing commands, and you can easily copy and paste.

Command line

Many early computers used a basic command-line interface (CLI). Instead of pictures and icons, only text is displayed on the screen, mainly because of the hardware limitations of early devices. Some of the earliest devices had no screen at all – the text output was printed on paper one line at a time.



The user had to learn and remember many different commands to perform basic tasks, such as creating files and folders (often called directories) and running a program. If one letter was typed incorrectly, the input could be rejected. Each command is typed in at a prompt, e.g. “C:”.

Menu-based

Menu-driven interfaces use a series of branching menus to navigate the system. These are used in modern desktop operating systems and older phones, iPods and MP3 players. The options can be selected by buttons, scroll wheels or touchscreens.

Adapted

An adapted interface can change depending on the device that you use, screen size or user preferences. For example, if you rotate a smartphone 90°, the screen changes from portrait to landscape and the position of the menu bar. If you plug a second screen into a laptop, the desktop environment changes to a dual-screen layout, or you may switch between a desktop and a mobile interface.

Some applications can adjust if you change the window size. Take a look at how the Microsoft Office or another package as you shrink and expand the window size. Or take a look at how a news website changes as you shrink the size of the browser – eventually the page will scroll horizontally.

Adapted systems may also allow customisation of the operating system to suit individual users. Fonts, colours and text sizes to be set by the user so that everyone can access the system.

Voice

In contrast to a graphical interface, increasing numbers of devices are capable of responding to the spoken word. Smart speakers operate nearly exclusively in this way, and many devices now support a voice interface, using a virtual assistant such as Apple’s Siri or Amazon’s Alexa to perform tasks.

Factors affecting the operating system

Choice

Most people use a GUI at all times (unless they’re occasionally using a specific device like a cashpoint, or an older device with an embedded system). The GUI is much easier to use than a CLI, and onscreen help functions when you hover over icons or buttons.

Most home users will use the version of the operating system that was preinstalled on their machine, usually Windows on a PC, or macOS on Apple-branded hardware. New versions of Windows and macOS are released periodically. Some PC enthusiasts might opt for a free upgrade to Windows 10, which was offered free to all Windows 7 and Windows 8.1 users. Some users will run a new version of Linux, or dual-boot two or more operating systems (selecting which one to boot), or will run ‘guest’ operating systems as a virtual machine in order to test new code.

Some businesses run specific versions of an operating system. In secure environments, updates and new versions will take place before rollout.

Most users will also use a multitasking OS as a result of running Windows or macOS. Some users will use a multitasking OS within limited embedded systems.

**COPYRIGHT
PROTECTED**



Performance

GUIs need many more computing resources than a CLI – faster processors, more graphics cards. They take longer to boot up than a very lightweight CLI.

While most consumers no longer use a CLI, they are still widely used by computer professionals as a powerful and quick way of performing tasks (you just type a few words rather than clicking windows and buttons) and for network administration. Additional letters after the command name are used to perform extra functions (called switches). If you're interested in taking a look at the help for a command, type the command followed by `/?` and you'll see a detailed help file with all of the options. For example, in both PowerShell and the older Command Prompt, `ipconfig /?` will show the help for the `ipconfig` command.

You can access a CLI in Windows (PowerShell and Command Prompt) and through macOS. Most of the commands are similar between the two systems with a few subtle differences. For example, in Windows, the command to check network configuration is `ipconfig`, whereas in Linux, it is `ifconfig`. Windows uses `\` within file paths, while Linux uses `/`.

Utility software

Purpose and features

Utility software is a general term for software that maintains your computer and optimises its performance (optimisation). These tasks generally run in the background. While their functions are built into the operating system, third-party versions are usually available. Examples include disk clean up, file compression, disk formatters and compression tools, backup software, disk repair and security software (antivirus and firewalls).

Choice and performance

While some users may be content to let the OS take care of itself (for example, automatically defragmenting the system and updating inbuilt security software), some users may decide to download or purchase additional utility software. For example, Windows Defender offers a basic free antivirus package. But to unlock extra protection, a paid-for package is required. A good antivirus package is required when you are handling confidential and personal data. However, any drop in performance is likely to be negligible.

Free versions of software are extremely limited, sometimes lacking basic functions. Paid-for versions are usually more feature-rich. Disk cloning software are particularly feature-light.

Application software

Purpose and features

Application software is any standardised software that we run on a daily basis to perform tasks on our computer. The software is usually purchased or downloaded from the Internet. It can be paid for (proprietary) or free (open source).

Examples include the Microsoft Office suite, or a free office suite, and web browsers such as Google Chrome. Graphic designers might use Adobe Photoshop or Illustrator, or specialist video creation software such as Premiere Pro or Final Cut.


Large software packages are feature-rich; thousands of tasks and options are available. For example, Adobe products. At university, one of my courses involved learning the basics of video editing. The lecturer said, 'We probably know how to use 10–20 % of the features. We'll only use about that 5 % we could do rather a lot with the software! It can be fun to explore the features.'

Utility software
performance
examples
and features

Application software
usage
examples
and features

**COPYRIGHT
PROTECTED**



example, you could play around with the different effects in a simple package such as Paint.net. If you haven't got access to Photoshop, you could try out GIMP (<https://www.gimp.org/>).  Go to zzed.uk/11526

Most users will be content with the standard 'off-the-shelf' software that's immediately available. All they have to do is purchase a licence and install it, usually from a download delivered instantly.

Choice and performance

Sometimes, the standard off-the-shelf software won't do – the situation is too unique, they regularly change or customise software; for example, in a bank or transportation solution is required – a very expensive option that could take months to create and a software team must be on hand to create, test and modify the software, and, of course, throughout its life. They will have to produce manuals and documentation on the software.

An advantage of using standard software is the level of support and information. Microsoft provides help pages and published resources to teach users to effectively use their software. There are thousands of forum pages and troubleshooting guides from Microsoft as well as Spiceworks, Stack Overflow and BleepingComputer, to name just a few that I've mentioned. They will provide email and telephone support, but you may need to pay for this.

There are lots of different options for software licensing. You and I might run software on two or three devices in our households, and the software might only be licensed for personal use. You might be able to install software on two devices but use only one device at a time (as with some mobile phone apps).

A business or an enterprise might use a volume licensing system – managing Office licences for hundreds or thousands of machines, often from a web interface, paying for the software per user or device. Volume licensing can be easy to manage and is scalable, meaning that you can add or remove licences as staffing changes, or add or remove features as required.

The more complicated or bespoke the system, the more training that users will need to learn the basic features of standard software.

Many of the larger software packages will run on both Windows and Macintosh systems, but some packages might only work on one, limiting the user's choice. The user might be limited by hardware. For example, Adobe Photoshop requires a graphics card for some functions (<https://helpx.adobe.com/uk/photoshop/kb/photoshop-cc-gpu-card-faq.html>), and only lists officially supported cards. Software generally has minimum requirements such as RAM. To run software at or near the minimum specifications, it could perform poorly; for example, the minimum RAM needed for Windows 10 64-bit is 2 GB, but 4 GB is recommended.

Mac users have had a lot of change over the past 20 years – as Apple transitioned from PowerPC to Intel (Apple Silicon) processors, from the classic Mac OS to OS X and macOS, and with the introduction of ARM-based systems. Apple has been criticised by some for discontinuing support for older systems.

Microsoft has had to maintain compatibility for the thousands of businesses that still use older versions of Windows. With this will change with Windows 11, we shall have to wait and see how it goes. The requirements and end of support for Windows 10 in 2025. Windows 8 gave us a lot of problems, but Windows 11 will be a winner. It is possible that Microsoft will relent on some of the requirements for Windows 11, such as opening it up to run on older processors.

**COPYRIGHT
PROTECTED**



Open-source and proprietary operating systems

All software has a licence that you must agree to in order to install it. That's the licence you say they've read and accepted without reading it. They can be very dry and lengthy and impenetrable to the average user.

The licence states what you can and can't do with the software in terms of installation and commercial use, whether you can copy or resell the software, reverse-engineer it, etc.

Open-source

Open-source software is free to use and modify. You can usually use it personally or commercially on any number of devices. You can sell your modifications, provided that the source code is provided for others to look at and modify.

Open-source – the software in which the source code is available and can be modified and redistributed. Examples include OpenOffice, Linux, etc.

Proprietary

Microsoft Windows and macOS are examples of proprietary software that are purchased from the company. You're not allowed to modify or reverse-engineer the software, and you are not given the source code to modify. There will be tight restrictions on the number of installations and often whether you can use the software commercially. When you buy the software, you might have different pricing options for personal and business use. Sometimes licences are fairly generic and just say the number of installations permitted by the version that you purchased.

Proprietary – the software is owned/licensed by the company and cannot be modified or reverse-engineered. Examples include Microsoft, Apple, etc.

Features of user interfaces

The user interface is important because that's what we look at all day. Sometimes there are many different versions of a program, but the one with the right features and most intuitive interface will usually be the best.

Software that has a clean, consistent and helpful interface is often the easiest to use. Mobile apps are generally a simplified version of the desktop versions – they have to be due to the smaller screen size.

In recent years, businesses have simplified some of their logos, and the icons used in their software packages. Take a look at https://logos.fandom.com/wiki/Microsoft_Windows to see how the Windows logo has changed over the years.

Microsoft has changed some of the icons in Windows 10 over the years to be more consistent. The icons used in its Office applications are very consistent – this makes it easy to switch between them. The introduction of the Settings menu in Windows 10, while the older Control Panel was still available, was a significant change. The same functionality is available on both systems, which look very different. Over time, users have moved towards the Settings menu in preference.

**COPYRIGHT
PROTECTED**



File types and formats

We store our files using various extensions that determine the type and structure of the file. Below are some common file types.

Images

There are a number of different file formats used for storing image data depending on its use, and the types supported by a computer can vary depending on the software installed on it.

Some of the most common image file formats are described below:

- **TIFF** – Tagged Image File Format (TIFF) is commonly used within the printing and publishing industry, and typically results in large file sizes. Multiple layered images can be stored in a TIFF file and it employs a **lossless** compression method.
- **JPEG** – Joint Photographic Experts Group (JPEG) is a file type that was specifically designed for image compression. It is commonly used for storing images and displaying images over the Internet.
- **GIF** – Graphics Interchange Format (GIF) is widely supported online and commonly used for animations. However, GIF only supports up to 256 distinct colours and uses a limited palette outside this palette.
- **PNG** – Portable Network Graphics (PNG) was originally developed to replace GIF, offering features such as transparency and **lossless** compression, although, unlike GIF, it does not support animation.

Video

A number of different video formats are used across the Internet to allow users to watch video content. The format used usually depends on a range of factors such as the type of video, viewing platform and expectation of quality.

- **AVI** – Audio Video Interleave (AVI) is a container format developed by Microsoft to play both video and audio. Advantages include its compatibility across a wide range of devices and Internet browsers, eliminating the need for specialist hardware. Additionally, it produces high audio fidelity and supports audio and video streaming.

- **MPEG4** – Moving Images Picture Expert Group 4 (MPEG4) is a widely used format designed to transmit audiovisual data, and can also combine the use of text.

One of the main advantages of using MPEG4 is that it produces high-quality, widely supported across websites and Internet applications, leading it to be commonly used for sharing and uploading video footage over the Web.

- **WMV** – Windows Media Video (WMV) is a video compression format originally developed by Microsoft. Its main advantages are that it supports the compression of large files with minimal loss of quality, and also results in small file sizes.

However, it does have compatibility issues with other computer platforms such as Linux and Mac OS.

- **MOV** – Apple QuickTime Movie (MOV) is a high-quality video format that's commonly used on Apple platforms. It can be used to store audio, video, effects and text (such as subtitles).



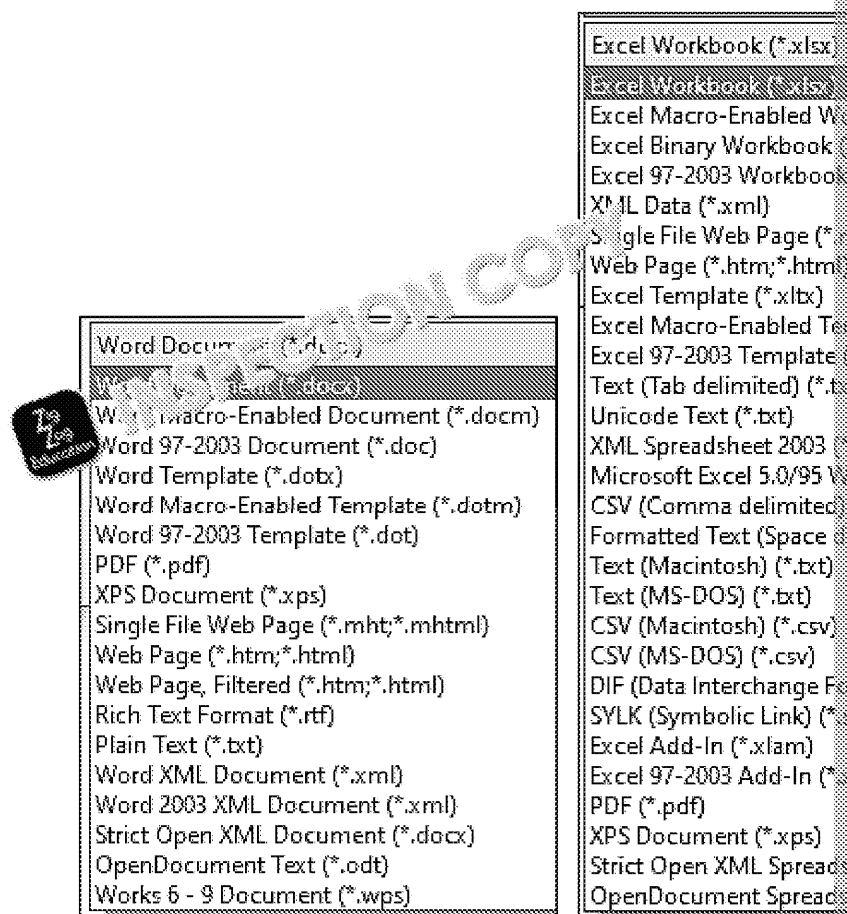
**COPYRIGHT
PROTECTED**



Application software

Where do you begin with looking at file formats for application software? There

A good place might be to take a look at the save options in a package such as Microsoft Office. You need to send your documents to others who use different software packages, which



Here you can see a huge range of different file formats (extensions) – some new, some old. Don't worry about the *, which just means any file name before the extension. Some of the newer formats like .xlsx are essentially proprietary to Microsoft. The 'x' is short for XML, a markup language that describes the internal workings of the files. If you're really interested in how a Word document is saved, open a file and change the file extension to .zip – you'll see a complex folder structure that is used in the document.

Of course, the actual program is saved as a *.exe file such as WINWORD.EXE. This is how you can run it (execute it). Some older DOS programs might be created as .bat (batch files). On the Mac, programs (applications) are sensibly named *.app.

Selecting file types and formats

Software packages like LibreOffice and OpenOffice, may be able to read documents created by other software to a degree of success – often formatting and styles change. However, the open formats aim for better compatibility between different software. CSV files are often used to exchange data between different software packages. Saving plain text removes the formatting.

If you're a Mac user, you may be familiar with the .pages and .numbers extensions, but not those using Microsoft Office though!

PDF (Portable Document Format) is a great way of sharing documents exactly how they look. You can create versions where you can add signatures and signing, but they generally

COPYRIGHT
PROTECTED



The issue of file compatibility is one reason why businesses tend to use standard software (moving between companies should be relatively familiar with the software).

Sometimes, however, there are issues with opening files created in different versions of software. For example, opening files created in a newer version within an older version. Sometimes files are saved in older versions. Sometimes we need to save a file in an older format, but some files created in the newer version will be lost.

An interesting conundrum is the issue with archiving – making sure that we can access our data in years' time. Software, and the computers on which they run, are ephemeral – they change. As software is replaced with newer versions, companies go out of business, and unsuitable hardware is replaced. Sometimes we can emulate older systems and software on modern systems, but it is not always possible. Files are lost if not converted to newer formats and onto newer storage media. Take a look at <https://aliciapatterson.org/stories/online-archiving-closing-its-memory> which was written about a recent new problem! Perhaps saving important data as PDF, plain text and commonly used image formats would be a good idea.



Questions – A3 Computer software in an IT system

1. Give an example of a type of operating system that would be unsuitable for daily office tasks, and explain why.
2. Explain why a computer is essentially unusable without an operating system.
3. What is the difference between utility software and application software?
4. Explain why open-source software is more versatile than closed-source software.
5. Which type of image file is used by consumer-grade cameras? Explain why.



**COPYRIGHT
PROTECTED**



A4 Emerging technologies

Affecting the performance of IT systems

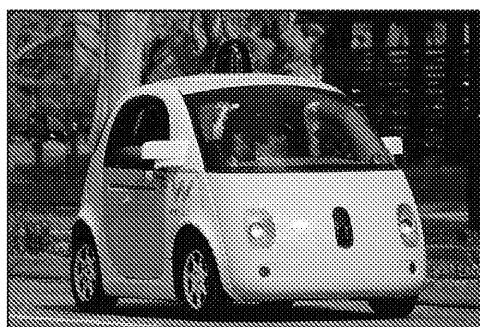
It's hard to believe how much technology has impacted and transformed our everyday lives, from the way we work, communicate and entertain ourselves, to our economies. The first computers only started to come into homes and businesses during the 1980s, and even the Internet didn't take off in homes until the late 1990s. The Internet has become pervasive. Social media and video-sharing sites have given us vast insights into other cultures. Want to try a recipe from somewhere else? Sure, and at least we can find out how much flour is in a 'cup', or the weight of a 'stick' of butter.

Here are some inventions that have, or will, literally change the world.

Autonomous robots

Unlike industrial robots, which simply repeat set instructions over and over, autonomous robots have a degree of intelligence, are able to detect changes in their environment and often have wheels or legs to move themselves around, and may sense people and objects and move out of their path to avoid collision. They may be used in industrial settings where the product differs slightly, such as picking items from shelves or storage, in cleaning (e.g. robotic vacuum cleaners), in space and in military applications such as unmanned vehicles.

Autonomous vehicles



Self-driving cars have been the stuff of science fiction, but now they are now a reality. You've been teased with different shapes for a while – how many different shapes can you complete where it asks you to identify traffic lights and even palm trees? Devices have been proposed since the 1920s, in the form of cars controlled or run on special tracks. The first self-driving car was built by the Carnegie Mellon University. Since then, many companies have started developing commercial products.

Now most car manufacturers are developing such vehicles, with increasing amounts of autonomy in recent years. Testing self-driving cars has been legalised in a few specific states where there is a human on board who can immediately take over if there's a problem. Most vehicles still have human control at times; a truly autonomous vehicle wouldn't even have a steering wheel.

There are lots of ethical and moral questions over the use of driverless cars, which would respond in the event of an accident (potentially without a human to kill), attempts by hackers to control vehicles, and a future population that has never learned to drive.

The first death from a driverless car occurred in Florida in 2016. The car did not respond to – a white truck that crossed the road.



Virtual reality (VR)

Since the 1990s, there have been many advances in VR to the mass market; for example, the Oculus Rift was released in 1995. The simplest and cheapest form is to use a smartphone mounted inside a cardboard or plastic head mount that uses lenses to focus your vision on the screen and uses

Em
pla
us
be
ad

Aut
ab
des



COPYRIGHT
PROTECTED



little more than the movement of your head for control. Over the last decade, more developed such as the Oculus Rift, HTC Vive and PlayStation VR, which use a powerful computer for the image processing, and usually some sort of handheld controller in addition.

You are probably more familiar with the social and gaming uses of VR; you may have seen videos on YouTube designed to be watched on VR headsets.

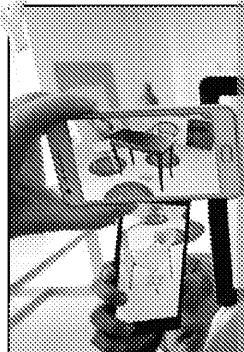
VR is used in many industrial applications, such as training (e.g. military parachute simulations, or by surgeons to practise operations in a safe environment without patients), in health treatments, sports training and also in teaching, usually with extra equipment.

One of the drawbacks of VR is the high cost – for both the headset and the computer or gaming PC needed to drive it.

Augmented reality (AR)

Augmented reality is taking a live image of the real world and overlaying digital objects on top of it. For example, you could use an app on a smartphone or tablet to create the image and then add digital elements on top.

One of the most famous uses is in the game Pokémon Go. Retailers have also produced AR apps, such as IKEA – you can place virtual furniture into your home to help you decide what would look good, as well as clothing and cosmetic companies, allowing you to see how you look wearing different clothes and make-up. Other uses include children's games and colouring books. It is also possible to use AR for promotion, such as providing images that start a video playing in place of the image.



Other AR systems project words and images onto a see-through helmet, visor or 'heads-up display' view used in many video games). This second concept has seen Google Glass, and other companies have developed or are developing applications for fighter pilots, for the battlefield, and consumer uses such as ski goggles.

We have only just scratched the surface of VR and AR here – the future possibilities and many new ideas will evolve as the technology further develops.

Artificial intelligence (AI)

Artificial intelligence (AI) is an attempt to mimic thinking, problem-solving and decision-making by a computer as if it were a human. The AI is given a large dataset in order to process decisions. Early examples of AI include simple chatbots and chess-playing computers. We use AI when talking to smart speakers, getting recommendations from Spotify, and using the help functions of some websites – they look online or at a database to come up with the best answers.

There are lots of advantages and disadvantages of AI. Advantages include taking over jobs from people (automation), which can save businesses money. They can also work available in all time zones. AI is often paired with robots, taking away dangerous jobs used in manufacturing, such as screening for cancers and diseases with a video. AI has helped give Stephen Hawking a voice.

However, disadvantages include that employees need to retrain or learn new skills for technical jobs; this can even be true in the creative industries, which were thought to be safe from automation. Where humans are replaced with AI, the personal connection is lost. High development cost. Hawking often spoke about the advantages and dangers of AI. The horror sci-fi films of AI taking over humans are a bit far-fetched, but we do need to think about future AI applications.

**COPYRIGHT
PROTECTED**



Machine learning (ML)

Machine learning (ML) is essentially a subset of AI. ML uses algorithms (sets of instructions for recognising and 'learning' new patterns in data. We give the algorithm sample data (like those pictures of traffic lights and trees we train driverless cars with), and over time it gets better at recognising them. This way the algorithm is capable of recognising patterns, avoiding pedestrians and trees, etc.

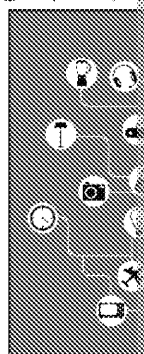
Another example of machine learning is the YouTube algorithm – its goal is to recommend videos that it thinks we want to watch, and promoting certain channels and individual videos. It also learns to recognise human speech and learn which emails are spam in order to send them to a junk folder.

One step further is deep learning, which uses neural networks – connections that mimic the structure of the human brain.



Internet-enabled hardware and the Internet of Things (IoT)

The **Internet of Things** (IoT) has grown rapidly in recent years. The definition of IoT is very broad – it includes a very wide range of smart devices that are connected to, and accessible over, the Internet, and can often be controlled through a smartphone app. The number of IoT devices is likely to skyrocket with the advent of the 5G mobile network. Devices are often wirelessly connected to home Wi-Fi or by other wireless methods, and include many devices such as kitchen appliances, smart speakers, doorbells and locks, baby monitors, electricity meters, colour-changing light bulbs, medical devices, smoke alarms, motion-activated cameras, and smartwatches and fitness trackers, etc.



There are many benefits to smart devices; for example, convenience, time-saving and ease of use. You can pull into your driveway, open the garage door, unlock the front door to your home and turn on the lights before even leaving the car. If you're going to come home earlier or later than expected, you can turn on or off the heating remotely. If someone delivers a parcel, you can speak to the delivery person and tell them where to leave it, and you can watch the delivery via a live video feed. You can also detect motion when nobody is supposed to be in.

Some of the major problems are security and lack of privacy – many of these devices are not secure and are a target for hackers (it has been shown that some cameras and baby monitors have been hacked). Manufacturers are starting to implement standards to improve safety, but this is a challenge because so many manufacturers are small businesses and end users can simply buy online and have goods shipped directly from countries overseas. Many of these devices send data 'home' to the parent company, which could be located on the other side of the world. Even when you are simply walking down the street may be seen and recorded by dozens of cameras. These devices can be tricky to set up securely, and many users won't take precautions like using a secure Wi-Fi network or regularly updating the firmware (e.g. patches to fix weaknesses in the software).

**COPYRIGHT
PROTECTED**



Personal use of IT systems

Which uses of emerging technologies are you most looking forward to using?

Perhaps it's exploring new worlds in VR, or purchasing your first driverless car in

As you progress through this course, jot down new technologies that you come across from them the most – businesses, or individuals like yourself?

IT systems in organisations

A fundamental change in business could be the use of VR in training and simulation learning to automate production processes in more efficient ways. In some cases, machines, while the more laborious or boring tasks further supplanted by machine new technologies could be very high.

Take a look at this video https://www.youtube.com/watch?v=ssZ_8cqfBIE which shows a delivery robot for groceries for delivery. That technology has been cheap to design and install!

Question A4 Emerging IT systems

1. Using an example, explain what an autonomous robot is.
2. Explain one ethical implication of using autonomous/driverless cars.
3. Give one use of VR in business and one in entertainment.
4. Explain why driverless cars need reference material to learn from.
5. Explain why there are security concerns over the IoT.

**COPYRIGHT
PROTECTED**



A5 Choosing IT systems



Here's a fun task for you – ask your parents and grandparents growing up or working their first jobs with no access to computers or the Internet, or using horrendously obsolete standards. I have grandparents who were typists who typed letters and orders on manual typewriters. One or two corrected by a special type of correction fluid or sheet. If they made mistakes, they'd have to retype the whole letter on a separate sheet.

New technologies have the power to scare people, making them fearful that their jobs will be lost. We still see news articles to this day, and you've probably noticed a few as self-serve checkouts in supermarkets, and in libraries. During the 1970s, a deep fear that the UK was losing its competitive edge and modernisation was vital. The government led by Margaret Thatcher sought to address these issues – ICT was a key part of this. A Computer Literacy Project was introduced with a series of educational TV programmes to go with it – the famous 'Beeb' or 'Beeb' as it's affectionately known. Many of these programmes are available on YouTube if you're interested. As a result, a new generation of home computer users was born, many starting programming in their bedrooms. (UK programmes have since been broadcast abroad to this day.) The UK has largely transitioned its economy away from manufacturing and into services and knowledge industries, helped by advances in technology.

Most offices have fully computerised, with employees spending nearly their entire day sitting at a desk and looking at a screen (often two screens, or even three!). Computers have helped with efficiency – beforehand, changes were harder to make – agreeing a contract with a client could take months as changes had to be manually retyped and agreed upon, sometimes cutting documents with actual scissors and using glue to stick paragraphs and pages together – that's why we still use the term 'cut and paste'. Nowadays, those changes can be typed straight into the document, which can be emailed back and forth. Email has now generally replaced the fax machine, which was a brilliant invention in its day.



Uses and benefits:

- ✓ All word processing, documents, information systems and messaging systems. Templates can be used for frequently used documents, and paragraphs of text can be moved between documents rather than retyping.
- ✓ Mistakes and typos can be easily corrected.
- ✓ Planning, diary keeping and scheduling can be centrally managed and shared. Meetings can be easier to schedule.
- ✓ Information can be shared freely and cheaply including email and VoIP.
- ✓ Instant messaging and video systems can be even faster than email, and now several people can be in the same virtual room at the same time.
- ✓ Data such as contacts, calendar and email can be synched to mobile devices.
- ✓ Cheap communications with customers – less printing and postage fees.

Disadvantages:

- ✗ The whole office can be ground to a halt by a power cut, loss of server or Internet updates, data loss or corruption, or malware/ransomware attacks (see Section 1.2).
- ✗ Some staff will complain of repetitive strain injuries (RSI) and eyesight deterioration from equipment and staring at a screen for hours at a time.

**COPYRIGHT
PROTECTED**



- ✗ Computer equipment can cost a company thousands, if not millions, of pounds, especially large enterprises with thousands of PCs to manage and upgrade.
- ✗ Data storage devices and mobile devices can get lost or misplaced, and data encrypted or remote wipe can't be implemented.
- ✗ Sometimes there is too much information – users in large companies may receive emails each day; many won't be relevant to them.

When we design the new system, there is a lot to think about.

User experience

- Ease of use – simply, how easy the system is to use. Is it intuitive? Can users quickly pick up the new system without lots of training? Is the system easy for new starters? Is it easier to use than the old system?
- Performance – is the system faster, more responsive than the old system?
- Availability – do all staff have access to the files and resources they need? Is the system available when required? Can the system be accessed remotely by staff working from home?
- Accessibility – is the system adjustable so that it is accessible to staff with disabilities?

User needs

An IT system in a large business will be used by hundreds or thousands of different roles and specific needs that must be met. IT isn't limited to just an office – there are needs required in warehouses, manufacturing facilities, labs, control rooms and workshops. Different hardware and software needs such as 3D printers, barcode scanners and specialist software may be predominantly Windows-based, but the design department may use Apple. Some staff may require a powerful workstation, others a laptop to take to frequent meetings.

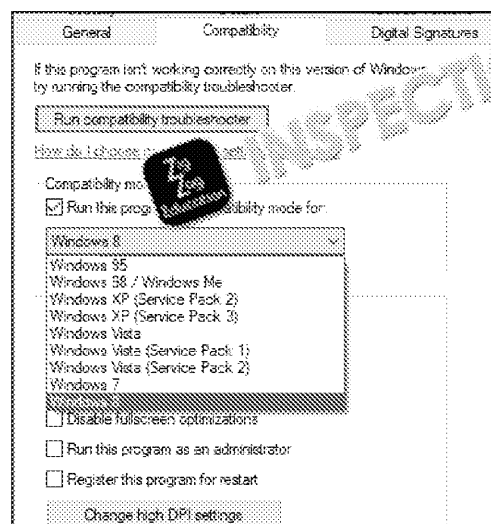
Some businesses use schemes such as *choose your own device* – staff can choose their own device, based on needs and experience level, usually from a predefined list. An example might be a smartphone and an iPhone.

Specifications

When planning a system, we will also need to choose the new hardware and infrastructure, and know the specifications – for example, we might specify the processor or amount of RAM needed in client machines, the requirements of new servers, or the speed and cabling types used in the network set-up.

Compatibility

Hardware – how much of the hardware will be retained? Will new hardware work with the old hardware?



Software – will the new software run on the existing operating system, or will the integrating operating system, or the operating system is upgraded? Will the software be moved to the cloud? If bespoke software needs to be developed, will be spent ensuring that all of the new software interface is appropriate.

Existing files must also be compatible with the new system – otherwise, years' worth of data could be lost.

**COPYRIGHT
PROTECTED**



Connectivity

Whether the existing network or Internet connection can handle new requirements, e.g. using cloud storage and computing; whether it needs to be replaced or upgraded with fibre or Cat 6 or higher cabling, whether there are enough wireless access points, and whether there are enough network sockets around the building, etc. The actual ports and wireless standards on the devices will need to be specified and compatible.

Connectivity – the methods used and capability of devices to be used with a network (e.g. Ethernet ports, Wi-Fi adapter), or cable (e.g. a USB printer or mouse)

Cost and efficiency

New IT systems can cost millions of pounds to implement in a large enterprise. The system operates well, and saves time (and, therefore, money) through increased productivity. An efficient system will be filled with intuitive shortcuts and templates, with pre-made reports. IT admins can set things up with a group policy.

Implementation

- Timescale – a timescale for the switch to the system will be established. This might include the planning, purchasing, installation, testing and training times.
- Testing – the new system will need to be tested before it is rolled out across a large organisation. Initially only a few users might have access to the new system – they can find problems and bugs which can be fixed before the system is rolled out to everyone.
- Migration – some staff may be reluctant to change, and all staff and management must be consulted and asked for their opinions because it's vital that they agree with the changes, can see the benefits and are willing to change. If the new system is not the old one, they might need a lot of training, possibly by the software company. Staff may even leave. Sometimes the old system will run alongside the new system.

Productivity

There is nothing more frustrating to the user than sitting at a freezing computer system, waiting for it to respond, or a crash that means that the last hour's work has been lost because the autosave function wasn't working. A fast and responsive system allows staff to stay productive. The new system should be as easy to use as the old one, if not easier.

Security

No system will be totally secure. The IT team needs to ensure that the new system is as secure as possible and meets all of the company's security policies and standards. Some companies invite hackers to attempt to hack into their systems in order to find and resolve weaknesses. This is called penetration testing, or 'pen testing' for short. New software must be checked for vulnerabilities and security updates and patches installed quickly after release. Large networks will use software that monitors the security of all of its devices to ensure that everything is secure.

Question Answering IT systems

1. Give two advantages of using IT systems in our everyday lives.
2. Give two disadvantages of using IT systems in our everyday lives.
3. Explain what is meant by the user experience of a computer system.
4. Why do additions or changes to a computer system require consideration?
5. Explain two aspects of implementing a computer system.

**COPYRIGHT
PROTECTED**



② B: Transmitting data

In this chapter you will learn:

- ① The different methods of connecting to wired and wireless connections
- ① The different types of network
- ① Why we choose different types of network
- ① Why different networks vary in performance

B1 Connectivity

A stand-alone computer has limited use. Even in the day, the average family computer was used for printing documents and homework, and playing games that arrived on a CD. Floppy disks were used to transfer data between devices.

But that all changed when we started to connect to the Internet – you could now receive email and download files. Early networks were hopelessly slow by today's standards, but fast enough to stream video.

Wireless and wired connections

There are many technologies that we use to connect out to the public Internet, and many networks in our homes and businesses. The most common methods are described below.

Most desktop and laptop devices have either an Ethernet adapter built into the motherboard or a separate network interface card. Most laptops, tablets, smartphones, smart TVs and game consoles have wireless receivers built in. In a laptop, the wireless card is connected to the motherboard and is located around the edges of the screen under the bezel. Some desktop machines also have wireless cards, but you can easily add one via USB if it doesn't.

Wireless

Wi-Fi (802.11 standards)

There are several different **wireless** technologies that use the 802.11 standards.

A **Wi-Fi** router takes the incoming cable Internet (copper, coax or fibre) into the home or business and broadcasts a wireless signal that you can connect your devices to. There are many devices that you can connect to Wi-Fi – phones, tablets, laptops, some desktops (all if you include a wireless card or USB adapter), TVs and a whole range of IoT (Internet of Things) devices, including colour-adjustable light bulbs.

Wireless
computers
linked via
the access
point

Wi-Fi –
devices

You might be surprised to learn that the name 'Wi-Fi' is meaningless – some people think it stands for 'wireless fidelity'.

In your home, Wi-Fi is probably built into the router provided by your Internet provider. You can use your own Wi-Fi transmitter and booster equipment, and add repeater devices. Multiple access points may be installed to ensure that the complete building has coverage. A single access point can support only a limited number of users with optimal performance. As you move around, your device automatically disconnects and reconnects to the next access point. Wi-Fi is used in many areas, including cafés, allowing greater work flexibility – from working off-site by video conference to informal meetings in the café itself.

Over time, Wi-Fi has improved in terms of speed and range. Most modern devices support both 2.4 GHz and 5 GHz technologies. Some networks can offer both frequencies in the 2.4 GHz and 5 GHz bands.

INSPECTION COPY

COPYRIGHT
PROTECTED



However, Wi-Fi networks can perform poorly, especially when the router is surrounded by other networks. If there are competing networks that overlap on the same 'channel'. You may notice slow speeds in certain parts of your home.

Wi-Fi is great because it allows a lot of flexibility on where you can work – very valuable in businesses where you can move around the building and attend meetings. Your device may even be switched to the different access points. But Wi-Fi isn't as reliable or usually as fast as a wired connection. Wi-Fi can also pose a security risk because it is accessible from outside the building – so make sure that you have changed the network and router's login password. Some companies don't allow staff to use public Wi-Fi to connect company devices for business use via public Wi-Fi over security concerns.



Mobile (4G/5G): Internet access either through your smartphone or via a dedicated mobile broadband (legacy), 4G or 5G network. Most of the time, you will access the data connection through your smartphone itself. Sometimes you might also 'tether' to another device which shares your phone's data connection to wireless devices such as a laptop, or through the USB connection.

You are limited to the monthly data allowance that is set in your phone contract – you might use the data very quickly if this is your only source of Internet access. You are also limited by the network signal strength where you live, which could be patchy in rural areas or even in densely packed cities.

4G (fourth generation) is the current standard for mobile Internet used in smartphones and some tablets. It is provided by cell towers used by telephone providers. It is currently being gradually replaced with 5G (fifth generation), which will offer greater coverage and much faster speeds (up to 10 Gbps), much lower latency, and less interference in urban areas because of the higher-frequency signals. But you will need to buy a new phone to get on to the 5G network, and the service is initially limited to larger towns and cities.

However:

- 4G signal can be patchy in rural and mountainous areas, and indoors as walls block signals. You'll have found this out when holidaying in the countryside.
- Calls and data connections can drop or time out.
- 4G routers are available which use a SIM card in the same way as a mobile phone (or fibre service). The data is then fed into your home's Wi-Fi network (and more recently some BT home routers) also have a 4G connection which switches over to if the normal cable Internet stops working, e.g. a fault on the line.

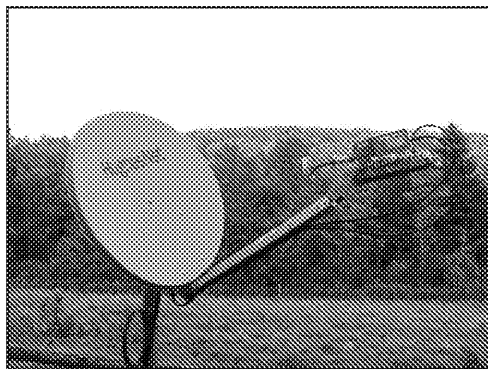
In the future, 5G routers could be a serious competitor to fixed home broadband and the Internet of Things.

Some people have protested over the installation of 5G and previous generations and how they fit into conspiracy theories: <https://theconversation.com/four-examples-of-how-coronavirus-conspiracy-theory-began-139137>

You may also be interested in reading about electromagnetic hypersensitivity: <https://slate.com/technology/2013/04/green-bank-w-v-where-the-electrosensitive-world.html>.

**COPYRIGHT
PROTECTED**





Satellite: if you live in a very remote area with no landline or mobile phone lines or there isn't a reliable mobile network, you can use satellite broadband.

You are probably familiar with, or have seen, satellite dishes attached to houses to receive TV. Satellite dishes can also be used to receive Internet access, but you also need to be able to send as well as receive. This requires geostationary orbit satellites, which are positioned far from Earth, meaning that they always stay in the same place.

Advantages and disadvantages of satellite

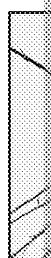
- ✓ Sometimes it's your only option!
- ✗ Very expensive compared to conventional Internet connections – perhaps £1000
- ✗ Typically slow (often 1 Mbps or slower)
- ✗ Often limited on how much you can download – perhaps a few gigabytes per month
- ✗ High latency – so poorly suited for some uses such as VOIP and online gaming

However, this could all change very soon. Elon Musk's Starlink project (owned by SpaceX) plans to launch thousands of satellites into space over the next few decades which will vastly improve satellite Internet, and at a more affordable cost.

Wired

Wired networking is generally the most reliable, but is more fixed. Typically, wired networking uses an Ethernet cable with an RJ45 connector on each end. Speeds are fast – usually 1 Gbps (Cat 5e). Some run at 10 Gbps (Cat 6). Ethernet cables use four pairs of wires that are tightly twisted together to reduce interference. However, each cable can only run for 100 metres. You can increase this if you use a powered device such as a switch between each run.

Wired – communications set-up whereby all data transmission occurs over Ethernet or other cabling



Broadband uses high-frequency wavelengths to transmit the data (outside of the range that phone calls can be made over the same cable at the same time. You may see a 'line filter' hanging from your phone line right next to the wall socket – one cable goes to the phone, the other to the router. This filters out the different wavelengths used by the phone and router so they don't interfere with each other.

To represent Internet on a copper phone line, think of a pipe with a small amount of water at the bottom – that water represents the voice frequency. There's a lot more room for the possible flow of broadband Internet data.

In the 1970s and early 1980s, the price of copper increased. This meant that some people started using aluminium instead. There are many online forums where broadband users compare the expected speeds compared to copper. It appears to be that aluminium is OK for higher-frequency broadband. No one in the 1980s could have predicted that.

Where the Internet access to your home, school or business uses an existing phone line, **ADSL** (asymmetric digital subscriber line) is the most common – asymmetric means that the download speed is much faster than the upload speed; for example, 20 Mbps download and 1 Mbps upload – OK for web browsing but not for uploading video, online gaming or having lots of people online at once. If you upgraded to use fibre, you'll get faster speeds, maybe 70 Mbps download, but you'll still have the same upload speed.

**COPYRIGHT
PROTECTED**



Some ISPs offer **SDSL** (symmetric digital subscriber line) connections where both download and upload speeds are the same. These lines are slow if using copper, expensive and rarely used today, but they are sometimes still used where extremely reliable connections are required. Some business-grade fibre connections are symmetric.

Broadband enables the user to have permanent connection to the Internet without losing access to the phone line or fax (as would happen with dial-up connection).

The fastest and most reliable connection is full **fibre**, delivered directly to your home or apartment block, which could offer you download speeds of several hundred megabits per second to a gigabit per second. You may get your Internet delivered through a coaxial cable (copper core) from an exchange that uses fibre – especially if you have a Virgin Media connection. Coaxial cables allow more data than a phone line – you might have a cable TV service where the cable splits in two – one to your TV box, the other to your router, which also support VoIP phones. Fibre connections are typically more expensive, and are not available in all areas.

The modern global Internet relies on glass fibre for its main infrastructure. This includes the cables that connect countries together. You occasionally see in the news that one of these cables is damaged by a ship, meaning that some countries' Internet connections will slow down until the cable is repaired.

Glass fibre uses pulses of light (e.g. a laser or LED – hence 'optic') to transmit data very rapidly at speed of light. This allows for a very high **bandwidth**, with thousands of connections over a single cable.

Bandwidth – the amount of data that can be transferred through a connection in a given time period (measured in bps)

Over time, the core copper network in the UK is being replaced with fibre – an expensive process as new trenches must be dug to lay the expensive cable.

There are two ways that customers benefit:

1. **Fibre to the cabinet (FTTC)** – the copper cable between the phone exchange and the street cabinet is replaced with fibre. You still use the same copper phone line from the cabinet to your house (the 'last leg'), but as there is less copper, the speed is much faster than ADSL – up to around 80 megabits per second download. Because you are still using copper, the speed varies due to distance as for ADSL – copper is definitely the weak point. Some companies provide Internet over a thicker copper cable (coaxial cable) to provide faster speeds than are possible on a regular phone line.
2. **Fibre to the home (FTTH)** – also called fibre to the premises (FTTP). Your home has a direct fibre network. As there is no copper, speeds are much faster (including upload) and you can pay for different speeds that the provider offers – a single person may pay for 10 megabits per second but a large family might pay extra for several hundred megabits per second.

Fibre rollout now covers much of the UK. It is expected that, over time, more homes will have access to fibre.

Advantages and disadvantages of fibre

- ✓ Very fast and low latency
- ✓ Much higher upload speeds – good for uploading files to cloud storage, or video streaming
- ✓ Tiered pricing allows you to choose a package to suit you
- ✓ FTTH allows you to stop using a copper phone line and paying line rental if you have a VoIP phone (and your router might allow you to connect a VOIP phone)
- ✓ Speed on FTTH doesn't slow down with distance from the exchange, unlike FTTC

**COPYRIGHT
PROTECTED**



- * Can be more expensive than ADSL
- * FTTH is not yet available everywhere
- * Maximum speed for FTTC is still reliant on the distance of your home from the exchange and your phone cable

The **Internet** is a network of interconnected computers which communicate globally using a unique (Internet Protocol) address. You may hear of the Internet as a 'network of networks' for both public and private networks, and commercial, academic, personal and government. Businesses connect their local networks in different countries via the Internet. Accessing the Internet enables a user to also access the World Wide Web (WWW) and other protocols which use the Internet for their transmission. The World Wide Web is a collection of websites which are available on the Internet.

The Internet is very useful in the home, school or at work – allowing the user to research information quickly and easily. You may use the Internet for research projects at school or college. Governments use the Internet to issue passports. The Internet can also be used for online banking so that you can check your account balance, request a statement and move money between accounts without leaving the comfort of your own home.

The Internet can also be used to:

- 🌐 **Communicate** – emails, chat rooms, social networks, etc.
- 🌐 **Entertain** – downloading/streaming music and video, online gaming, etc.
- 🌐 **Inform** – wikis, articles, blogs, etc.
- 🌐 **Shop** – for goods (e.g. clothes) and services (e.g. car hire)

Computers are networked together globally using telephone network technology over a phone line in the form of analogue and digital signals. Analogue is the standard for voice and is transmitted in varying waves. This makes analogue slower than digital and more prone to corruption. Digital data is transmitted as ones and zeroes and is constant. Digital data is transmitted faster than analogue.

The public Internet is made up of millions of different devices, all with specific functions. It is connected around between the Internet service providers (ISPs) and various types of servers, including web and DNS servers, which translate your request for a website into the IP address of the server. Data travels around the world as 'packets', through fibre-optic and copper cables that run along underground trenches.

An ISP (Internet service provider) provides an Internet connection for a monthly fee. Some ISPs provide cabling into your home if you're not using your existing phone line (e.g. fibre or coaxial). You may also need a router. There are many ISPs available, such as BT, Virgin Media, TalkTalk and many others. Each offers different connectivity services, at different prices and speeds. Where you live can influence the services available because of the local infrastructure. Some remote communities have chosen to set up their own, effectively becoming a small, independent ISP for a village or hamlet. An ISP provides:

- * Internet access
- * email and web space
- * online support
- * firewall protection, content filtering (e.g. parental control) and sometimes free antivirus software

**COPYRIGHT
PROTECTED**



The features of connection types

Individuals

In your home, your ISP will connect you to the Internet and supply you with a basic wireless built in, and four Ethernet ports. Some people may choose to purchase the

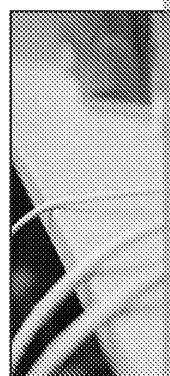
You'll connect with Ethernet cables to your router if you want a better connection than (latency) – great if your devices are in the same room, but not so great if you're in a different house. Some modern houses can be pre-wired with Ethernet for an extra cost, and so their homes with Ethernet cables that run through the loft or under the floorboards. There are also network adapters which plug into existing electrical sockets and use the electrical cables to transmit the data. Some powerline adapters also add an extra wireless access point.

Organisations

In businesses, all networking will be done in the walls or in trays near or above the ceiling. Cables are installed in the walls, trunking on floors, all leading to switches and patch panels. This is likely to be the case for new buildings, and has been 'retrofitted' (after being built) in older buildings. While many small businesses are wired with copper cable, large sites may use fibre-optic cable to connect their infrastructure together. This is because copper cable typically can't be run for more than 100m before the signal degrades. Once installed, the network devices such as PCs, laptops and tablets are connected to a nearby socket with a short cable.

Here are some examples of the networking equipment that is used on the Internet in homes and businesses:

- **Gateways** (sometimes called **routers** on home networks) – connect your private internal network (local area network, or LAN) to the public Internet (a WAN – wide area network), which both use different protocols. Gateways use a system called NAT (network address translation) to convert the addresses of your internal devices to the public address provided by your ISP.
- **Bridges** – connect two networks with the same protocols.
- **Switches** – either managed switches or unmanaged switches send data to specific devices on the network using the MAC address of the device. They form the backbone of the network.
- **Hubs** – similar function to switches but they send the same data to every device on the network, reducing the overall throughput. They have been largely replaced by switches because of this limitation. They are often used as a 'hub' with the routers that are provided by ISPs such as BT and Virgin; they are used to connect multiple devices to the Internet.
- **Wireless access points** – deliver network access to many devices over the air.
- **Clients and servers** – clients are any computers on the network that receive data (they request the data); for example, your PC is the computer that you sit at and request web pages and data. A server is locked away elsewhere in the building or is in the cloud. It stores data and pages to the client when requested. Clients process and use the data. Servers also host applications that are viewed on the client through a web browser.



**COPYRIGHT
PROTECTED**



Selecting and using different connection types

For the incoming Internet connection, there might be no choice or lots of choice. FTTC has been installed.

Internally, most businesses and homes will use a combination of wired and wireless. The network may be wired, but wireless available for laptops and mobile devices to connect.

Here are some advantages and disadvantages of wired and wireless connections.

	Advantages	Disadvantages
Wired	<ul style="list-style-type: none"> ✓ Fewer interruptions to signal ✓ More secure ✓ No health concerns about exposure to radio waves ✓ Fibre-optic cables provide faster broadband speeds where available 	<ul style="list-style-type: none"> ✗ Wires are messy and prevent connecting multiple devices in rooms in a household, or in a business ✗ Unshielded cables are susceptible to interference in some instances (instead if that's an issue)
Wireless	<ul style="list-style-type: none"> ✓ Ease of use, no wires ✓ Devices identify and connect to each other without needing physical attachment ✓ Mobility and outdoor use: can connect to the Internet via public Wi-Fi hotspots 	<ul style="list-style-type: none"> ✗ Possibility of a break in service or interruptions in service (power outages) ✗ Less secure, limited range ✗ Using higher-consumption devices and most, but not all, devices are not energy efficient ✗ Other wireless devices can interfere with the signal ✗ There are health concerns about wireless radio waves and their effects on the human body

The performance on the IT system

The performance of a network is affected by lots of factors, including:

- the speed of the Internet connection (in megabits) and the latency – fibre vs. copper, the exchange
- the type of cabling within the internal network, and equipment – some older speeds of 100 megabits, versus 10 gigabits
- the number of users downloading and uploading files at the same time, or streaming
- the number of users connected to a wireless access point
- distance from the wireless access point
- the mobile signal strength and whether connected to the 2G/3G/4G/5G network, and signal quality

Questions – B1 Connectivity

1. Give one advantage and one disadvantage of using wireless Internet standards.
2. Which type of Internet connection might you have to use in an extremely rural area?
3. Fibre is often used instead of copper cable. Give two examples where this might be used.
4. Explain the function of the router in a typical home network set-up.
5. Explain why the type of network connection impacts the performance of a network.

**COPYRIGHT
PROTECTED**



B2 Networks

Features of the different networks

There are many types of network, ranging from one person to a home or an office that spans several countries.

Personal area network (PAN)

A small network consists of the devices owned by one person. They have a small range, perhaps 10 metres, and can either connect a bunch of devices together, or one device can provide a connection to the Internet. Examples of a PAN include:

- a printer plugged into a laptop
- speakers, headphones, keyboards or (photo) printers connected to a laptop or smartphone using Bluetooth
- file transfer between a laptop and a smartphone over Bluetooth or infrared
- tethering a smartphone to a laptop using Wi-Fi, Bluetooth or USB. Tethering is a connection with another device, but the data used counts towards your mobile data allowance.

Personal area network (PAN) – small-scale wireless set-up between devices owned or operated by a single person, e.g. by tethering several devices from a smartphone or using Bluetooth.

Local area network (LAN)



A LAN is the network in your home, or in an office building or campus. The internal LAN is connected to the Internet via a router.

In an office, the LAN is often set up in a star topology. Servers on the network are set up to provide access, login, shared printers and sometimes file storage.

In the home, you are typically connected directly to the router. You can connect to other devices in a peer-to-peer fashion; for example, share files between computers, stream files to a smart TV.

If you think that LANs are just for the home and office, think again! Take a look at <https://www.guinnessworldrecords.com/world-records/116433-highest-altitude-lan-party> and <https://www.youtube.com/watch?v=OPYvCdgZmgc> – a group of people who made a Guinness World Record for hosting the world's highest altitude LAN party on Mount Elbert in Colorado.

Wide area network (WAN)

A WAN consists of two or more LANs that could be located in branch offices around the world. Each LAN is connected to the Internet via a router and they connect to each other across the public Internet. WANs are useful because they allow resources and servers to be accessed across the different sites, for example, served from the head office.

Virtual private network (VPN)

You are probably aware that VPNs exist – the companies that provide them often sponsor technology-themed YouTube channels. VPNs provide a secure network 'tunnel' over an insecure public network, including Wi-Fi in a coffee shop, and the public Internet.

Businesses love VPNs because they allow cheap and secure remote working and business flexibility. A business may set up its own VPN server which the remote workers connect to. All of the network traffic is encrypted to travel over the Internet and the remote laptop or device, through the router on both ends.

**COPYRIGHT
PROTECTED**



Some individuals choose to encrypt their network traffic in a bid to increase their security. However, using a public Wi-Fi connection an attacker on the network could see which websites you visit because modern sites use HTTPS, and your ISP (Internet service provider) can't see your traffic. However, the benefits of using a VPN may be overstated in some cases. Take a look at <https://www.youtube.com/watch?v=WVDQEoe6ZWY> to learn more. Because you are using a VPN provider, VPNs can be used to get around geo-restrictions, such as content that is only available in a specific country – if you are outside of the UK and use a UK BBC iPlayer abroad, that wouldn't otherwise be allowed.

Factors affecting network choice

There are many factors in the choice of network – such as a LAN, WAN and VPN. In your home, just by having an Internet connection, your router will automatically connect to the router a private IP address (e.g. 192.168.0.3). The router shares the Internet connection. You can also connect to other devices on your home network, such as printing.

In your school, college, or in a business, there are many more services available, such as file sharing and often an email server; however, some of these services are now rapidly changing. The choice of networks will be determined by the needs of the business – if there are remote employees, a VPN will be set up. If there are no remote employees, then a VPN will not be set up. In a business, data is backed up from one location.

User experience

The experience will usually be based on speed and latency. The experience can be affected by the network and the Internet connection. The network must be easy to use, perform well (be reliable), and should be available whenever a user needs them, and the network should be accessible – in the building, or off-site.

User needs

The users will usually need a fast and reliable Internet connection. The firewall must allow specific traffic that they need, and not block any necessary websites. All cloud services and resources should be available whenever needed, including access to required files. Staff training might be necessary after an upgrade to the network. Staff must be consulted about the upgrade, and timescales should be established.

Specifications

The network manager will carefully assess the needs of the users and any extra requirements, such as carrying traffic to the backup system, and peak demands as users log in. The network manager will monitor use, ensuring that upgrades to the network are sufficient to meet demands. For example, if the company is forecast to grow to about 70 staff who need a VPN, the firewall must be capable of allowing at least 70 VPN connections, and the network must be able to allow for further expansion. They will also ensure that the upload speed is sufficient to support a large number of VPNs.

**COPYRIGHT
PROTECTED**



Connectivity

To an extent, the incoming connectivity choice is limited to the types of cabling including upload and download speeds. Internally, connectivity is determined by sockets in the walls, and wireless access point. Large networks are likely to use a as a client-server relationship, while smaller networks may operate in a workgroup.

Internal networks also have different structures, called 'topologies'. A star network devices are directly connected to this. If the central switch fails, the whole network the equipment branches off. Each room or department is fed from a separate switch switch). If one of the switches fails, only the devices connected to the one switch.

Ad hoc networks can be very unreliable if the mobile signal drops or if the device the hotspot.

Cost

The price of Internet connections varies. Full fibre and leased lines can be very expensive. Internet. An ADSL connection running over the copper phone line can be very cheap backup Internet connection.

Networks vary in cost based on their size; the number of cable runs and drops to fibre is used internally (expensive) and whether Cat 6 cable is used (more expensive). switches, access points and servers will vary from network to network, and the price quality and specifications of the network. A tree network uses more cabling and Ad hoc networks are much cheaper to set up.

Efficiency

A fast, optimised network that is easy to use will allow users to be efficient. They without the wait of files to download from the Internet or from the file server. This to save a large Word document and having to wait 10 seconds every time you print over a VPN.

Compatibility

Any upgrades to the network must remain compatible with existing infrastructure. networked devices are still in use that use the 802.11 g (or earlier) network standard. access points must support backwards compatibility. Some older devices may also authentication (e.g. WEP) which should ideally be replaced with devices that use.

Implementation

After the chosen network has been specified, it will need to be purchased and set occur outside of normal working hours (e.g. at the weekend or overnight). This is switched off in the process (which would cause major disruption to the business), testing to ensure that it is working as expected. Any downtime (including from re-kept to a minimum.

Productivity

Again, a slow system will reduce the productivity, or the amount of work that the could occur if an important service was down for several hours or more – if the is working, or if a file server goes offline, then staff will have to resort to backup methods. Cloud services could be lost, unless a backup connection was used to restore a if comes back online, any data generated will need to be manually entered into the.

Security

Generally, a wired connection is more secure than a wireless connection. This is be accessed from inside the building. A strong wireless network can usually be accessed signal strength on some wireless access points can be reduced. When setting up a passwords should be set, and the incoming connection should have a firewall installed unknown sources. Servers should also be secured, and file access controls set up, if

**COPYRIGHT
PROTECTED**



How features and components affect the performance of a network

Internal networks work well when there are fast internal connections, such as fibre optic cables, between the networking equipment. Some servers and switches can increase the number of or more data links between them; for example, two network cards within a server. If a network (e.g. 100 Mb/sec) is in use, then transfer speeds are low – for example, when operating on a cheap, poor-quality Ethernet cable can reduce performance.

A fast fibre Internet connection, including an expensive leased line (e.g. 1 Gb/sec with low latency) will make cloud storage and applications very responsive. A fast upload and download connections and file uploads perform well. A fast upload speed also allows the business to upload large files. A slow ADSL connection shared between many users will perform poorly.

Questions – B2 Networks

1. How do WANs and LANs vary?
2. Give a business advantage of using a WAN and explain why it is an advantage.
3. Give two legitimate uses of a VPN.
4. Explain how cost will affect the choices made when implementing a network.
5. How does the failure of a network affect productivity?

COPYRIGHT
PROTECTED



B3 Issues relating to transmission of data

Protocols

Protocols are easy to understand once you break them down.

A **protocol** is a set of rules that govern how data is transmitted between different devices over a network (servers, clients, routers, etc.). Each method of communication, such as web traffic and email traffic, uses one or more protocols. The Internet also uses its own suite of protocols: TCP/IP (Transmission Control Protocol and Internet Protocol).

Data is broken down into small chunks called packets. Think of them as envelopes containing letters that are delivered through the mail. Each packet is addressed to travel across the network across any available path, and they all get reassembled at the other end in the correct order. For example, different packets of the same file could travel through different routes and even through different countries!

In electronic communications, a protocol specifies the format and headers of the packets should be sent, and whether error-checking is used (i.e. whether the packet uses the Datagram Protocol (UDP)). If we need all data to be delivered, we use TCP, which ensures packets are received correctly (and, if not, the packet is resent). Live audio and video streams use UDP because there is no check for whether packets go missing – they can't be resent because the stream is live.

When data is transferred using a protocol, a port is opened up. Each port has a number and is used for one or more specific ports, or use one that's not already in use.

So imagine that you're having a conversation over the phone with a friend. One of you initiates the connection by dialling a number, and you will both use a shared language, such as English. You speak at a certain speed, and if you mishear something, you'll ask the other person to repeat themselves.

Email

Emails are sent between email servers running special email exchange software. You can access your email either through a web browser, such as Gmail, or through a desktop 'email client', such as Outlook or Windows Mail.

Email – electronic communication method where text, HTML and attachments are sent to someone with a valid address via mail servers



Several different protocols can be used when sending and retrieving mail between email servers.

Often you can access your email from both a web browser and a desktop client.

If you only access email on one device, you might use a protocol called **POP** (Post Office Protocol version 3) is the most commonly used version. The email is transferred to your device from the server. However, if you want to access your email on several devices, then you need a better solution. If you choose to use POP, then only use one client, and remotely access your email from other devices.

IMAP (Internet Message Access Protocol) is a better solution because the emails are transferred to any number of devices and email clients. If you use the Gmail app, emails are downloaded using IMAP. They remain on Google's server and you can still access them from another client.

We send emails using **SMTP** (Simple Mail Transfer Protocol). Emails are sent from your email client to an email server. The emails are then transferred between email servers to the recipient's email server.

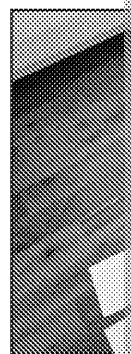
**COPYRIGHT
PROTECTED**



Voice and video calls (VoIP)

Voice and video calls are sent over VoIP (Voice over Internet Protocol). They can be received between client software or web browsers running on computers and laptops, and apps on tablets and smartphones. Some offices also use phone handsets that

Voice and video calls (VoIP) – sending real-time audio communications over the Internet (rather than using a telephone service), e.g. apps such as Skype, Zoom, Teams and FaceTime, or using dedicated telephony hardware



use VoIP instead of older analogue systems. VoIP is very cheap to set up, but you do need a fast and low-latency Internet connection, and may need separate speakers, a microphone or a webcam if these are not built into the computers). Video calls and conferences between many users (sometimes thousands) would be very difficult on an older phone system.

VoIP services usually have a central server to manage the connections, through which they are sent. Examples include Teams and Skype from Microsoft, and Zoom. Basic accounts are free, but more advanced accounts can be expensive – they may have more features built in, or allow more minutes of use per month. Some VoIP services can receive and make calls to the traditional telephone network.

If you want a really in-depth look at VoIP, watch this video: <https://www.youtube.com/watch?v=...>

Web pages

Web pages are displayed in a web browser (although you probably already knew that). The pages are written in a language called HTML (hypertext mark-up language). The web browser requests the page, and the HTML code is delivered, which is the instructions for how to display (render) the page. The code includes all of the text, and specifies how it should be formatted, along with images and their size, etc.

There are two main protocols used to request a web page. HTTP (Hypertext Transfer Protocol) is the unsecured version, while HTTPS (HTTP Secure) is used today for most websites (e.g. online shopping, banking and webmail, etc.). Using HTTPS encrypts the network traffic, so that it would be unreadable to a hacker.

Secure payment systems

Online sales, banking and money transfers using the Web use the secure HTTPS protocol noted above. This encrypts all of the card and transaction details. Transactions may require additional security measures, such as sending one-time passcodes to a phone number linked to the account, or using a card reader (see section D2 for more on two-factor authentication).

You can often pay for items in a retail store using your smartphone or smartwatch using contactless authentication of the payment. This uses a secure protocol called NFC (Near-Field Communication) in conjunction with an app, e.g. Google Pay (Android phones) and Apple Pay (iPhones).

Many bank cards also have an RFID (radio frequency identification) chip built in, which emits radio signals in order to make contactless payments. Cards also contain the older technologies of an embedded microchip (the gold part of the card) and still a magnetic strip.



**COPYRIGHT
PROTECTED**



Security and considerations when transmitting data over different types of network

Open network connections don't need a password to connect to, and they're still open. If we don't know who the network belongs to, or if the network is open, then we need to be careful when connecting. A hacker could set up their own network with a similar wireless name to the one we are connecting to. All connections made (called a man-in-the-middle attack), and if no password is used, the traffic between your device and the router is not encrypted. A legitimate open network is fine, but if you're still using HTTP sites, then it is probably worth using a VPN. Some businesses have a policy in their IT policy that states that employees are not allowed to connect company business activities over an open network.

Bandwidth and latency

The amount of data (technically the frequency range) that a cable can transmit is called bandwidth. The larger the bandwidth, the more data that can be transmitted in a second. We refer to this as 'gigabits per second' – the number of bits carried in a second. A gigabit is 1,000 megabits.

We often use the term 'bandwidth' to mean the speed of our Internet connection. If an Internet service provider promises up to 20 megabits download speed, you can download 2.5 megabytes per second – as there are eight bits to a byte.

One older type of Internet connection was ISDN (Integrated Services Digital Network). It was a slow speed, so some people joked that ISDN stood for 'It Still Does Nothing'!

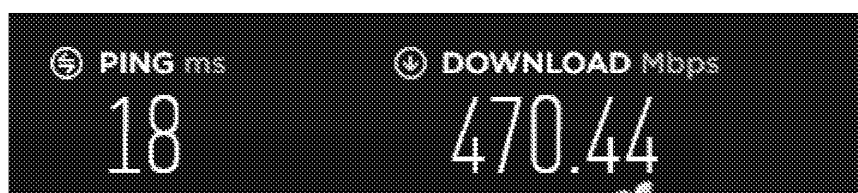
Latency is the time it takes for a packet of data to be transferred across a network. We measure latency in milliseconds. The lower the latency (lag time), the better, and the more responsive. For example, imagine trying to control a remote system where there is a second or so delay – that would be very high latency (1,000 milliseconds is one second).

Bandwidth – the amount of data that can be transferred across a network (in bits per second). It is measured in megabits per second (Mbps) or gigabits per second (Gbps).

Latency – the time it takes for a request to reach a server and for a response to be received – a similar concept to delay.

Factors affecting bandwidth and latency

Here you can see the results of running an Internet speed test. The connection is rated from the ISP at 500 Mb/sec download and 50 Mb/sec upload:



What can we tell from it?

- The ISP is using fibre within its network, so the download is too fast for ADSL line, so we are using either FTTC or FTTP with a coaxial cable.
- This is not a satellite connection.
- The internet network is running at a speed of at least 1 Gb/sec.
- This connection is asymmetric (the upload speed is significantly slower than the download speed).
- This will be a fairly expensive connection.
- Other users are accessing the network, either internally or externally, because the ISP aims to provide. The test could have been performed at a time of day, for example, when lots of people are connected to a VPN or are streaming video.

**COPYRIGHT
PROTECTED**



So a summary of the factors is:

- Bandwidth of the cable type (as well as incoming Internet speed from the supplier)
- Distance from the exchange – higher latency and slower speed with further distance
- The type and speed of the external connection.
- The load on the network – high when logging on in the mornings, or when many users are online

Implications and performance

Internet and network speed is essential for large enterprises where hundreds of services – downloading or uploading files at the same time, or connecting through the Internet – are used. It has been discussed the time wasted, frustration and drop in productivity caused by a slow network.

Connections to web pages can easily time out if the speed is slow, especially on long distance connections. Latency connections can make VoIP difficult.

Compression

Compression describes the process of gaining an accurate representation of data while maintaining acceptable quality. The reduction in file size allows more files to be sent or downloaded over a network connection.

Lossy and lossless

Lossy compression removes data, and quality is often reduced.

Lossless compression, however, reduces the file size without any loss of quality due to the use of patterns. The file size of a file compressed using lossless compression is smaller than that of the original, but using lossy compression would create a far smaller file.

Lossy – type of compression that removes unnecessary data at the expense of quality. For example, MP3s can sound different from the original audio file.

Lossless – files are compressed into a smaller space, without any loss of data. The data is then decompressed into its original form. Lossless compression algorithms are used for files where quality is important.



You can see the effects of lossy compression in the image.

COPYRIGHT
PROTECTED



Applications and implications of data compression

The technology used to compress a RAW image (the file format normally generated by a digital camera) into a JPEG file is interesting, but is quite advanced. If you zoom in on a JPEG, the sharpness has been discarded), whereas if the file was saved as a PNG or a TIFF, then sharpness is preserved. Network Graphics – was designed to allow high-quality lossless images to be transmitted over the internet while keeping to a small file size.

One of the worst uses of a JPEG image is to save text as an image; this is because the text will be surrounded by other blocks of colour (called artefacts) surrounding them. You may have noticed that when a page containing text or graphics is uploaded to Wikipedia (rather than their preferred version, which is usually the notice asking for an SVG file to be uploaded).

Similarly, the lossy compression of an MP3 audio file allows for small downloads and also server space. Mobile devices often have limited storage, meaning that the audio files must be small there too. However, if too much data is lost (in a process called sampling), then the quality of the audio is lost.

Use of codecs when using and transmitting audio and video

A **codec** is a program that is used to code and decode (hence the name codec) an audio or video data stream, and can compress the data using either lossy or lossless compression. The actual compression and decompression is done by an algorithm within the software. Most video applications have commonly used codecs built in, but if you try to open a file that uses an unusual codec, then the appropriate codec will need to be downloaded, often automatically after prompting the user. Many of the codecs, while lossy, can retain much of the quality. To save bandwidth, newer codecs have been developed for streaming services.

Codec – computer software that compresses and decompresses audio and video data for transmission (audio, video, etc.).



MP3, for example, is actually a codec! A standard DVD uses a codec called MPEG-2. There are also codecs for broadcasting, such as digital video.

Some audio (including in videos) is normalised, which means that the volume is consistent across all parts of the audio. There are no parts that are louder or quieter. It would be annoying to need to constantly adjust the volume while listening, or between tracks and videos. For this reason, YouTube applies normalisation to all videos.

Questions – B3 Issues relating to transmission of data

1. What is meant by the term 'bandwidth'?
2. Which protocol is used to transfer email FROM a server TO a client machine?
3. Give two examples of when VoIP might be used.
4. How can online payments be made secure?

**COPYRIGHT
PROTECTED**



③ C: Operating online

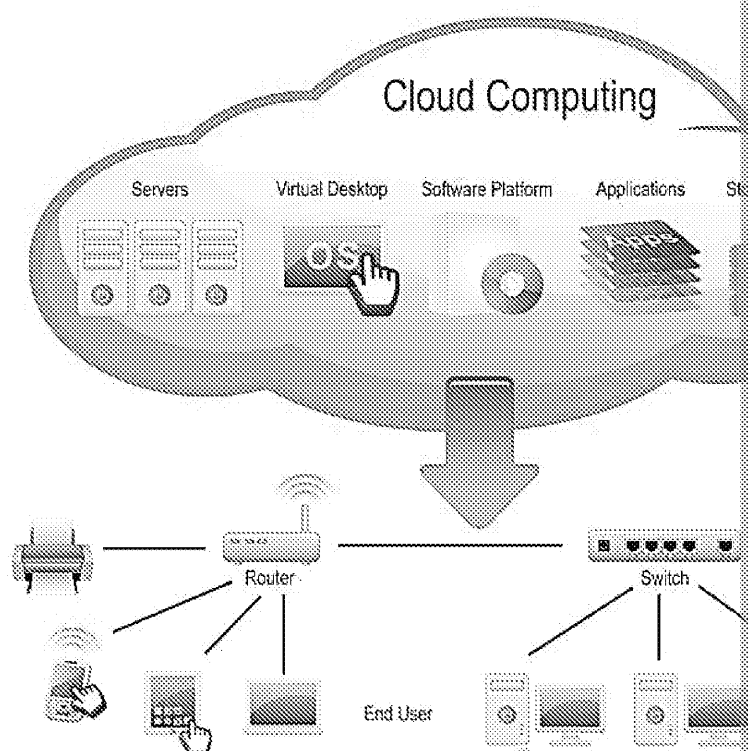
In this chapter you will learn:

- ① The uses, costs and benefits of cloud storage and computing
- ① Ways that we use to communicate online both personally and in business

C1 Online systems

In recent years, businesses and consumers have started to move away from on-premise systems to online file storage and cloud computing. You have probably used cloud storage if you have a Microsoft account comes with 5 GB of free OneDrive space. Operating systems and applications are stored on servers, providing access from anywhere in the world.

Cloud computing is often used for virtual computing, such as software and other services, which are hosted on the powerful hardware of a shared remote server and accessed via the Internet.



Cloud storage

Instead of having on-premises servers (the traditional method of storage), many businesses are now storing their files on 'cloud servers'. The term 'cloud' represents the idea that there are millions of servers that are connected to the Internet.

Cloud storage
Internet, e.g. Google Drive

These servers are located in special buildings called 'data centres' that house thousands of servers. These buildings have fast Internet access and consume a lot of energy for air conditioning – those servers pump out a lot of heat. They are kept very cool.

Setting up a cloud storage account is very easy – usually you just apply through a website and choose the amount of storage that you need. Some companies will give you a small amount of free storage on a personal account, you just need to use the password you choose. In a business scenario, you may need your own login, and may only be able to access certain files.

**COPYRIGHT
PROTECTED**



Synchronisation

Sometimes you have a copy of files on both your device (e.g. laptop) and in the cloud. If one copy of the files changes, then that change gets copied to the other location.

For example:

- You can work on your laptop – when you save or modify the file, the new version is copied to the cloud.
- If you work on the file online, or someone else with shared access works on the file, the modified file is copied over to your device from the cloud.

This service needs an active Internet connection. Synchronising can be very useful if you work without a connection – just work on the local copy, and it will be copied back to the cloud when you have Internet access.

You can share files with other people by providing an appropriate share link. They can then access a folder – this is great when people are working with the same files and always need the latest version. This stops people from working on different versions – which wastes time and messes up the data.

Cloud storage can be accessed from anywhere in the world providing there are no restrictions are set, the files are accessible 24/7/365.

Cloud computing

An example of online software is Microsoft Office 365, which provides the newest online versions of traditional Office programs, such as Word, Excel and Access, to multiple PCs or mobile devices. This provides a flexible way of using and sharing resources and can be utilised in the home, in small or medium-sized businesses and in schools and universities. An annual or monthly subscription fee is incurred for access to the online software; this typically allows usage on several PCs or devices, and the need for local storage is reduced. Cloud computing enables users to quickly create documents and share documents online.

Cloud computing allows applications and hardware to be accessed via the Internet.

An advantage of this software over stand-alone software packages, such as Microsoft Office, is that users can create, edit and share documents on a variety of PCs or mobile devices using the Internet. Access to the newest versions of software provides greater functionality and capabilities. The ability to share and store documents online, helps to increase productivity and output.

Remote backup services, also referred to as digital vaults, are provided by Internet service providers. For an Internet connection for a fee, providing convenient access to files over the Internet. Users can share files with friends, family or colleagues via a password.

It also allows a user to protect their files by enabling automatic backup. For data security, files are not recorded on a single device or confidential or sensitive data.

The benefits include:

- **Low up-front cost** – it can be shared across a network of computers and servers rather than per user, unlike traditional software licences
- **Low maintenance** – the vendor rather than the client deals with issues
- **Mobility** – the client can access the software from anywhere
- **Instant availability** – because the software is not installed physically onto a device, the software is immediately available to the client
- **Automatic backup** – files are automatically backed up onto online storage

**COPYRIGHT
PROTECTED**



Comparing the different types of cloud computing

Infrastructure as a Service (IaaS)

IaaS uses virtualisation technology to deliver the cloud computing infrastructure storage (hard drives) and virtualisation.

The service provider of the cloud servers provides a dashboard (or an API), giving control over the entire infrastructure. IaaS provides the same technologies and as a hosting company without having to physically manage all the set-up and maintenance.

The subscribers have to install and maintain their own operating system, middlewares and applications. Although the subscribers have control over these, with this comes responsibility for security and updates, which requires considerable knowledge.

Examples of IaaS providers are Amazon Web Services (AWS), DigitalOcean, Microsoft Azure Compute Engine (GCE) and Cisco Metapack.

Platform as a Service (PaaS)

PaaS delivers a framework for developers that they can build upon and use to create applications. PaaS service providers include everything in IaaS (network, servers, storage and virtualisation) plus the operating system, middleware such as programming languages, and runtime environments. PaaS also provides special software components to support programming development. This means a development team can concentrate on programming their own applications without getting involved in the hardware and set-up of the servers.

The IaaS service providers above also provide PaaS, and others include Oracle Cloud PaaS, IBM Cloud Platform and Red Hat OpenShift.

Software as a Service (SaaS)

SaaS is software that runs from the Internet rather than from individual computers. A common example of traditional software is Microsoft Office, which can (at the time of writing) only run on an individual computer, compared to Microsoft Office 365, which is the SaaS version of Office which can be run from any device using a web browser.

SaaS has some brilliant advantages over traditional software:

- ✓ Accessible over the Internet
- ✓ Subscribers are not responsible for installing the software or for dealing with updates
- ✓ It has a central management console
- ✓ Hosted on a remote server so there are no hardware or installation/maintenance costs

However, there are some disadvantages too:

- ✗ SaaS applications are often not integrated with existing software or other resources
- ✗ SaaS applications often have fewer features than installed software
- ✗ It is often much more expensive with monthly charges rather than a single one-off purchase
- ✗ It is much more difficult to guarantee that data is not accessed by the service provider or other users such as GDPR (e.g. at the time of writing, no EU company can use Google Analytics because it transfers data out of the EU to the USA without their consent, and the now defunct Privacy Shield).
- ✗ Minimal customisation is possible as subscribers cannot install anything.

**COPYRIGHT
PROTECTED**



On premises	IaaS	PaaS
Application	Application	Application
Data	Data	Data
Runtime environment	Runtime environment	Runtime Environment
Middleware	Middleware	Middleware
Operating system	Operating system	Operating system
Virtualisation	Virtualisation	Virtualisation
Server	Server	Server
Storage	Storage	Storage
Network	Network	Network

Key:



Administered by customers ↑
Administered by providers ↓

Impact on individuals

Individuals can use cloud storage to save files when using multiple devices, and family. Cloud computing allows friends and family to collaborate on and edit documents simultaneously. For example, a group of friends could be playing an online quiz, score for each round in a spreadsheet, or several people could mark up a calendar up. Online webmail takes over the requirements of needing a desktop email client.

A very useful feature of cloud storage is the upload of photos from a smartphone synchronised to other devices, and also acts as a backup if you lose your phone.

Remote working has huge benefits and gives individuals greater power and flexibility to commute to work, or allowing more flexible hours that could better fit around child care. It also allows working from home and working in the office – part-time for each and provides the benefits of face-to-face social contact. Even before the coronavirus pandemic, many people began to work from home part-time. In some cases, this was negotiated in lieu of a company policy that working from home was allowed for perhaps one day a week. Some companies had a company policy that working from home was allowed for perhaps one day a week. Some companies had a company policy that working from home was allowed for perhaps one day a week. Some companies had a company policy that working from home was allowed for perhaps one day a week.

However, remote working is not for everyone. During the lockdowns of 2020 and 2021, many people worked remotely for the first time, and often not out of choice. For some of them it proved to be a challenge. The daily interactions with colleagues, particularly for less experienced employees, and the mentoring that happens in an office environment.

Watch this space over the next few years – it's likely that millions of people have been forced to work remotely. Companies that force a rigid in-office approach could have difficulty retaining staff. And while some people are finding they want a remote or partly remote job, others are looking for a non-remote job.

**COPYRIGHT
PROTECTED**



Impact on organisations

Imagine that a company has an on-premises server that is getting full.

They can either:

- Buy larger disks to install in their server. This requires lengthy copying of data to the new disks (perhaps several days), and a trained technician to set it up.
- Purchase a second server that could cost thousands of pounds as a one-off expense (requiring a technician to set it up).
- Migrate to a cloud server and switch off their on-premises server.

On-premises servers require ongoing maintenance (and the associated costs) and a constant supply of electricity. This is included in the price for cloud storage.

With cloud storage, the amount of storage can be varied – by paying more to increase the storage, and by paying less if less storage is needed. This is called scalability. Instead of a big one-off investment in hardware, monthly or annual fees are paid, and are appropriate to the current needs of the business.

We can also use software in the cloud. Instead of a program installed on your computer, the software is stored on a remote server, and just access it on your device – often through a web browser.

Cloud computing makes the software much easier to administer:

- Just select and pay for the software that you need (just like cloud storage) and the number of users. Increase and decrease as the number of staff changes (scalability).
- No lengthy installations on thousands of machines throughout an office building.
- Everyone is using the same version of the software – no incompatibility between versions installed or licensing issues.
- No need to push out security updates or upgrades – this is all handled behind the scenes by the software company.
- You can use less powerful and, therefore, cheaper hardware in the office – all that is needed for is to act as a screen, provide keyboard and mouse input, and display the results. The processing is completed on the powerful server.

But there are drawbacks, such as:

- Some online versions of software have fewer features than the desktop version.
- Needs a stable and fast Internet connection – otherwise the application will be slow.
- If the Internet connection is lost or down, then the software is not accessible. Compared with on-premises servers, there is much less potential for downtime.

**COPYRIGHT
PROTECTED**



Below is a summary of the key advantages and disadvantages of cloud computing

Cloud computing (online applications)	
Advantages	Disadvantages
<ul style="list-style-type: none"> ✓ Cost-effective – it can be shared across a network of computers and some vendors charge for usage (including per hour) rather than per user, unlike traditional software licences ✓ Low maintenance – the vendor rather than the client deals with issues and provides updates ✓ Mobility – the client can access the software from anywhere ✓ Instant availability – the software is not installed physically onto a client's computer(s), but is made immediately available to the client via download ✓ Space saving – no physical storage space is required ✓ Accessible 24/7 from anywhere with an Internet connection ✓ Allows for flexible staffing and working from home 	<ul style="list-style-type: none"> ✗ Connection – affects performance and latency. If you lose access to the Internet, you will affect speed of the application. Usually slower than local applications ✗ Lack of control – the client has no control over settings/defaults ✗ Security – not protected by the same measures, such as firewalls, as local software; the server is accessible to anyone with the right access ✗ Outdated – the version on the remote server might be outdated
Cloud storage (online files)	
Advantages	Disadvantages
<ul style="list-style-type: none"> ✓ Ability to share files with other users ✓ Ability to access files wherever you are and from a variety of mobile media (laptop, smartphone, etc.) ✓ Some vaults use encryption to protect data ✓ Frees up storage space on your computer ✓ Not affected by the corruption of physical storage media ✓ Some providers automatically back up files 	<ul style="list-style-type: none"> ✗ Confidential or sensitive data is at risk from hackers (but it could be encrypted and especially on a secure connection) ✗ Data not protected by the same measures (such as firewall and antivirus) as local data ✗ Data not backed up by the provider ✗ Need an Internet connection to access the files (and could be slow) accessing files at a distance

Enabling and supporting remote working

In addition to cloud-based offerings, the following technologies enable remote working

VPNs

We've already discussed the technology behind a VPN – the secure network tunnel that provides secure data transfer to and from the office, meaning that a laptop connected can access all of the resources, files and folders as though it were inside the building.

Remote working
when not in the office (e.g. a public office (mobile office))

An employee might be given a company laptop which they can connect directly to the office. But they can also take the laptop off-site and connect via the VPN. On the laptop run as normal, but loading times might take longer depending on the speed in the office, and the download speed of the remote Internet connection.

In a corporate setting, the VPN connection on the laptop will have been configured by the IT department. In a home setting, anyone can set up a VPN connection from their device, as long as they have valid

INSPECTION COPY

COPYRIGHT
PROTECTED



Remote desktop technologies

Unlike a VPN where you use locally installed apps, a **remote desktop** connection is essentially an image of a remote computer screen that is streamed to your device across an internal network, or over the Internet. You use your local keyboard and mouse for control, and can sometimes share printers and the clipboard. All of the software you use is installed on the remote computer, not your own. This means that the local device could be a cheap, low-powered model, called a thin client. If the network connection is fast with low latency, then the experience of using the remote desktop differs little from using the machine locally.

Remote desktop component allows access to a different screen of a different computer work off-site or on a network.



There is a remote desktop client built into Windows (and also available on Mac). To view a remote device, but the remote device must run either the Pro or Enterprise edition of Windows. There are also third-party remote desktop connections available, and designed to work across many devices, including to Windows Home edition. Some remote desktop connections are designed to be used through a web browser. Take a look at <https://remotedesktop.google.com/>

Uses of remote desktop:

- Staff remotely connect to their normal computer while working off-site; for example, a teacher might connect to their classroom computer from home.
- Staff could remotely connect to a machine that is running specialist software that is not available on their local machine.
- Staff or students could log in to a profile on a server (doesn't require individual accounts on each machine).
- A computer technician will often remotely connect to servers for configuration or to troubleshoot a user's PC while providing technical support.

The use and selection of online systems

When selecting an online system, there are lots of considerations. For example:

Security

The system needs to be at least as secure as the existing on-premises system. This means that the system must be able to store and protect commercial data, and protect against threats such as hackers and malware. We'll discuss data breaches later. Ideally, staff should only access online systems on company equipment, and security can be controlled by the employer. Increased wireless provision in schools is a risk, if poorly implemented (e.g. if an unsecured guest account is left active). With remote access, some staff may not follow security protocols as rigidly! It is estimated that the risk of data breaches increased in 2020 because of the sudden switch to home working.

By outsourcing data storage and backup to an external company, security could be improved. However, many businesses do not have the time or expertise to invest heavily in on-premises security, and security can occasionally be neglected because it doesn't make the company any more profitable.

Cost

Online systems have the ability to save money due to less on-premises hardware and software options. Cheaper on-premises equipment can be purchased, and staff productivity is increased. However, nowadays with GDPR, data breaches can be very expensive!

Ease of use

As we said with IT systems, a system that is easy to use will often be the winner. Simple systems require less training and are quicker to use.

**COPYRIGHT
PROTECTED**



Features

The business will need to choose a system with enough features, but not needles. Unlike a bespoke piece of software, online systems are off-the-shelf packages. He will use a tool that allows extra features and software packages to be added and

Connectivity

Broadband Internet connections are now commonplace in homes and businesses, remote working and access of cloud-based services. In 2020, around 97 % of homes had broadband Internet.

Questions – C1 Online systems

1. Why might cloud storage work out to be cheaper than an on-premises server?
2. How does cloud computing provide flexibility to businesses?
3. Explain one advantage of using online backup for mobile devices.
4. Both VPNs and remote desktop connections are used for remote working, how do they differ?
5. Which is more secure – storing data on a mobile device or storing data on a cloud server?

INSPECTION COPY

COPYRIGHT
PROTECTED



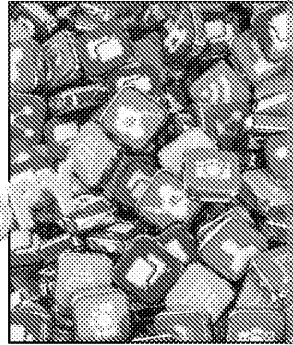
C2 Online communities

Communicating and interacting with online communities

There are many platforms that we can use to communicate online.

Social media

There are many social networking sites; for example, Facebook, Twitter, LinkedIn, Snapchat, Instagram and TikTok. These types of site provide features such as forums, instant messaging and file sharing, which allow you to post information about yourself and communicate with other users.



Social networking has impacted how people socialise.

It is now possible to communicate and share

information with people from different backgrounds, cultures and countries with ease. Many of the benefits are obvious – more social interactions (even if not face to face), the ability to organise meet-ups with friends or like-minded people, the ability to keep up with

However, friends made via social networking can differ from the usual definition of friends. A large number of them may be true friendships. It is important to recognise the difference between genuine and when unscrupulous people try to form friendships with other users by creating a fake profile (profile), such as using a false identity, gender and age. Users can gather friends' personal information, video, audio, photographs and links with other users via their personal profiles. It is important to keep your profile private and only visible to friends and family to prevent fraudsters or hackers from accessing your personal information. A public profile should only be used to communicate with friends that cannot be used to identify you.

Participants can comment on their friends' profiles on a comment space, wall or timeline, which is visible to other users who have access to that profile.

- Be careful what you write about other people.
- Be careful what information you give away about yourself.

Information that you post on a social network space will be visible to other users. Think about this before you add anything you may later regret; for example, photos of a night out or a potential employer.

Information can also be copied and pasted into other areas, so you never know where it will end up. Embarrassing photos or videos could turn up on YouTube to haunt you.

Social networking sites enable others to see what you are doing and where you are.

INSPECTION COPY

**COPYRIGHT
PROTECTED**



Social media	
Description and purpose	<ol style="list-style-type: none"> 1. Facebook – good for staying in touch with family and friends and following businesses and joining groups of like-minded people. 2. Twitter – short microblogs, good for keeping up with news that you follow. 3. LinkedIn – the professional social network where you build your skills and past employment – a bit like a CV (in fact you can see what recruiters that you are looking for work). You can endorse your skills, contact potential employers, and view job postings. They can also contact you directly. 4. Discussion boards (forums) – some are about a certain topic and knowledgeable (and not so knowledgeable!) people reply to your posts.
Accessibility	Each platform has its own set of accessibility features.
Advantages	<ul style="list-style-type: none"> ✓ Can stay in touch with family and friends ✓ Easily follow businesses (businesses can use social media to generate sales) ✓ Can be used to find new employment ✓ Start discussions with like-minded people ✓ You can get free help and advice on issues that you have
Disadvantages	<ul style="list-style-type: none"> ✗ Need to be very careful what you post publicly. Need to consider the consequences. ✗ Social media can be addictive, waste time and cause stress. ✗ Can work against you in employment – do you want a full of bad posts? ✗ The people who you chat to online might not be who they seem. ✗ Public groups can get nasty – offensive language and trolling.

**COPYRIGHT
PROTECTED**



Blog, microblog, vlog

Blogs are diary-style journal entries posted onto a website such as WordPress, or smaller sites for niche or specialist interests. A blog usually takes the form of a series of entries, with the most recent entry at the top; it comprises text along with photographs, and sometimes drawings and video frames.

People may be willing to share details about their lives, their opinions, experiences and travel. For example:

- A travel diary for a once-in-a-lifetime trip so that friends and family can read about their adventures
- A day-to-day diary for followers and fans
- To document and review new purchases, life, vlogs, health and fitness changes, food, DIY and craft projects etc.
- To showcase interests such as photography
- To discuss opinions, views and events

Businesses also set up blogs to generate consumer interest and provide details of developments, or upcoming product launches.

Blog
writing that is
business

Micro
writing
popular

Vlog
YouTube
about
week

Blogs, microblogs, and vlogs	
Description and purpose	<p>Blogs are often short diary-style entries provided on a web page first. They are typically hosted on platforms such as Blogger or WordPress and photographs.</p> <p>An individual might write a blog documenting a travel adventure or share recipes and experiences.</p> <p>Businesses also use blogs to provide updates to their customers or announce product launches.</p>
Accessibility	<p>Blogs are usually simple web pages that are easy to read and have simple buttons to view the next or previous pages, and may have a search bar.</p> <p>The blogs can be short, and written in simple language – but they may not have been proofread, and English, for example, might not be the first language so some blogs may be difficult to understand.</p>
Advantages	<ul style="list-style-type: none"> ✓ Great for families and friends to keep up with those going away ✓ Can be used to showcase skills, good for landing new jobs ✓ Easy to read, often very entertaining ✓ Useful for customers ✓ Useful for businesses to promote products in a more personal way
Disadvantages	<ul style="list-style-type: none"> ✗ The blogs can be read by anyone in the world – they might give away too much personal information – they know the user's name and address is empty ✗ Readers may get bored if there are long delays between posts

**COPYRIGHT
PROTECTED**



Microblogs are much shorter and are often used to share updates, opinions and news. The most famous microblogging service, where each post is called a 'tweet' and is limited to 140 characters, is Twitter. That longer posts need to span several tweets. Individuals can set up an account, and those with the most followers tend to be celebrities, including musicians and sportspeople, political leaders, and large companies.

For example, in August 2021, 30 of the top 50 followed accounts were of American people on Twitter were Barack Obama (former president of the United States); Justin Bieber (musicians); Cristiano Ronaldo (footballer); Taylor Swift, Ariana Grande, and Selena Gomez (musicians and/or TV personalities); and finally YouTube at number 10.

Donald Trump, during his presidency from 2017–2021, was well known for his use of Twitter as a medium to bypass the official communication channels. He was eventually suspended from the platform for tweets surrounding events where protesters stormed the US Capitol building. You can find more information at <https://blog.twitter.com/en/topics/company/2020/suspension>

Vlogs are 'video blogs' and are uploaded to sites such as YouTube – they are videos of a person's life, what the vlogger does at weekends, a day in the life, hobbies or holidays and so on. Vlogs can also be uploaded to TikTok. Some vloggers provide extra vlogs for fans who pay to subscribe to them, or money through Patreon. This is in addition to the advertising revenue gained from receiving such attention and comments can be mentally damaging.

Wiki

A **wiki** is an online repository of information that has many authors. Pages or articles are created for each topic, which are linked together. Perhaps the most famous example is Wikipedia, an online encyclopaedia. There are over 6 million articles written in English, with almost 54 million articles across all languages. This is a fantastic knowledge base; however, not all of the pages are always accurate or unverified data. Because anyone can edit it, the platform is constantly changing.

Wikis are set up for niche hobbies and interests; for example, a wiki for all of the details of a computer system. Businesses may also set up wikis as a type of training or help system for an intranet, designed to be accessible whenever staff need it.

Chat rooms

A **chat room** is similar to instant messaging (below) – a space for people to discuss a topic in real time by typing comments and replies, or over VoIP, with others. Some chat rooms allow strangers to meet; sometimes they will chat online for years and get to know each other well, and can form life-long friendships. But there are also dangers of online chat rooms – people may hide behind a screen name and not be who they say they are. One popular service is Discord – many YouTubers have set up discord servers, allowing followers of their channel to chat about the topics that their channel is based on. In the past, IRC (Internet Relay Chat) was a popular method of communication online.

**COPYRIGHT
PROTECTED**



Instant messaging

Instant messaging (IM) is immediate and enables users to identify whether another user is online; it is a low-cost means of instant communication between two or more users. Instant messaging also allows users to communicate for free over the Internet and use webcams to transmit real-time images and transfer files. IM is a great way of communicating via simultaneous conversations, providing speedy communication and ease of use. The benefits of instant messaging are:

- Conversation is immediate and performed in 'real time' (unlike email)
- The environment is controlled (users need a user name and address or IM address to take part)
- Pictures, photos and files can be exchanged
- It is cheap and easy to use

Instant messaging – short pieces of text, images and audio that are sent in real time between individuals and groups, but are also used in corporate settings to replace reliance on email

IM can be performed via peer-to-peer (P2P) transmission or via a server-client network (the server receives the message and retransmits the message to the recipient). Most modern IM services use strong encryption to keep messages private. In some cases, not even the messaging provider can decrypt the message.

There are a wide number of instant messaging clients and apps available on smartphones and tablets. You are probably very familiar with services such as Facebook Messenger, WhatsApp, and Telegram.

Podcasts

Podcasts are usually audio files (occasionally video) that an individual or business uploads to a podcast for immediate download, and are played whenever is convenient to the listener.

An individual might produce a podcast about a topic that interests them perhaps every two weeks or once a month.

A business might release frequent podcasts as a cheap and fast method of providing information to customers.

Benefits of podcasts include:

- New episodes are automatically downloaded to your device when they become available.
- Don't need an Internet connection once downloaded.
- Can be listened to whenever convenient, including while performing other tasks, such as commuting – when reading would be difficult.

Forums

Unlike a chat room, a **forum** is not conducted in real time. A user begins a new 'thread' about a particular topic or asks a particular question, and others post comments in an attempt to answer the question or share their knowledge. Forums can be a useful tool for getting help; for example, if you are having a specific issue with your computer and can't find a resolution online.

Forums are often public and can be found through search engines. While most posts are helpful, you will also find some not-so-good advice, or advice that is incorrect or dangerous. Moderators can remove posts either by a human or using a program called a bot, that will remove spam or posts that break the rules. Most of the replies take place in the first few days or weeks, and, after a while, the thread is archived.

**COPYRIGHT
PROTECTED**



Implications for individuals of using and accessing online communities

Over the years, we have taken increasing advantage of online communities, from creating social media accounts, to posting in chat rooms, to listening to podcasts. Some of these activities now form a big part of our lives. However, because of the addictive nature and unhealthy, sedentary lifestyles and social damage that online communities can bring (fake news, misinformation and cyberbullying), some people have chosen to delete their online accounts and spend more time meeting people in person, or reading actual books.

If you have a smartphone, you might be able to track and see how long you've used it for and which apps you use the most – you might be surprised!

Here you can see that I used my mobile on Monday 16th August for about an hour – I spent about 20 minutes writing an email to a great aunt who was holidaying in Grand Canyon, and to my dad to arrange a drop-off of some family photos. I spent 10 minutes catching up with a few friends on WhatsApp, and took a bunch of photos myself (of slides from the 1960s). I used Firefox to catch up with the news at lunchtime. I've tried to use Facebook less, and it looks like I'm succeeding. Of course, this timing doesn't include the eight hours I sat in front of a computer screen at work, or the time I spent sitting at a computer in the evening scanning photos!

While social media can bring us closer together and allow us to get back in touch, there are many downsides in general. For example:

- Time! Social media is addictive and, before you know it, 10 or 20 minutes has passed and you've scrolled down your news feed.
- Mental health – remember that people only post online what they want you to see. Their apartment, their achievements, their latest purchases, their trips out and the like. However, just like your life, not everything is plain sailing. Don't feel jealous if you're not having a good time.
- Bullying and harassment – social media can be a channel for cyberbullying, stalking and other forms of harassment.
- Public profiles – check your settings to make sure they are set to private to protect your identity or using your photos without permission. For example, scammers will use your photos on websites using photos from random people's social media accounts. They then contact you and ask for money – they often pretend to be in the army because that's a profession you can't meet in person if they claim to be posted overseas.

User experience

Social media and other online platforms are typically easy to use and are available pretty much every platform. Most have a smartphone app and can be viewed in a web browser. Occasionally, services go offline, and millions of people grumble about that! For example, WhatsApp can very occasionally stop working for a few hours – typically used for social purposes, but a big headache for a business user.

Sometimes, using older hardware can be a problem. Smartphones can't always be updated to the latest version of Android or iOS, meaning that app support drops. For example, in 2021, Facebook had developed a 'lite' version of its mobile app, Facebook Lite, and Messenger. Originally designed for release in African countries where older or less powerful phones were used, they are available in other countries. They run much faster than the standard versions, but lack some of the features – you can't 'react' to messages, for example.

**COPYRIGHT
PROTECTED**



Meeting needs and accessibility

There are platforms and apps for just about anything, so we're well covered. However, accessibility – being productive online and keeping up with friends should be easy in 2020.

Social media sites have a wide array of accessibility features, and some can be used with a screen reader. Take a look at the accessibility features on the platforms that you use.

- Facebook <https://www.facebook.com/help/accessibility>
- Twitter https://blog.twitter.com/en_us/topics/company/2020/making-twitter-more-accessible
- TikTok <https://www.tiktok.com/accessibility/>

Cost

Many online services are free to use or have a free version available; for example, Google, Twitter and TikTok, etc. However, these services are funded by advertising and we are sharing our service with our data. Some podcasts are paid for, while the majority are free. But there is a fee for premium features. Some services have a free version funded by the paid-for version which shows adverts. You may have skipped past the pop-up asking you who the advertising partners are – it's a little scary how many other companies are advertising people about you.

Privacy

Privacy concerns keeping your personal data private. Anyone who uses an online service has a privacy policy and conditions that set out how that service processes and uses your data. We share our personal details online, through instant messaging and email, which could include whether we're in debt, or if we're depressed. Google's Gmail reportedly used to place ads based on the content of the email, but if the email appeared sensitive – for example, 'funeral' – it wouldn't start trying to advertise funeral directors and no ad would be shown.

It's astonishing how much information that we give away online – from the information in our posts, the things we like and dislike, etc. When all of this information is collected, a picture can be built up. You could take a look at how much information someone has shared on one of your social media accounts.

It's important to think about the personal data that we upload, and also we should check our privacy settings on our online accounts, making sure that our personal information is protected.

Security

We should keep our data and accounts as secure as possible as identity theft can happen. For example, if someone has taken out a credit card in your name. Always use strong passwords and two-factor authentication if possible. Can you imagine what could happen if your email account was hacked? You wouldn't be able to reset the passwords to all of your online accounts if they didn't need to be sent to your phone.

Implications for organisations of using and accessing online services

Online communities and social media is a lucrative business for many companies. Companies use social media for advertising, making customers aware of new products and updates, and customer feedback. Companies that they are interested in, Social media can drive customers to their website and leave favourable reviews.

Employee and customer experience

Many people now expect companies to maintain an online presence. For example, a company's Twitter account is invaluable to follow to find out which bus services are running and when.

Most customers will have a good experience of using a product; for example, seeing a product being used, or fun arts and crafts (even birthday cakes!) that use the company brand.

**COPYRIGHT
PROTECTED**



A fun example is Herdy, a company based in the Lake District, which sells sheep. <https://twitter.com/HerdyUK> or <https://www.facebook.com/HerdyUK/> – notice the same name, HerdyUK, for brand consistency. However, social media can be used in many ways, and not always in a public way.

Staff need to know how to defuse a situation, and many companies now use online as a way of communicating with customers and resolving problems.

Customer needs

Customers need and expect a fast and efficient service from a company. They will find a company through its online presence, such as a basic web search, meaning that it must be at the top of popular search engines. Companies need to ensure that their sites and content are accessible; for example, by providing alt text for screen readers to describe images, or transcripts for audio content.

Cost

An organisation's presence on social media sites might be free to set up, but there are other costs. The company may need to hire staff to spend time creating the social media presence, or it may outsource this to an external company. Jobs in setting up social media accounts were rare a few years ago, social media was in its infancy. Now, social media advertising courses are readily available. Companies may need to train existing staff, use the service of consultants, or hire new staff with specific skills.

The beauty of social media is that advertising can be targeted to very specific demographics. Ads can be seen by thousands of people very quickly, unlike a billboard advertising campaign. The more specific the company wants to target, the higher the fees paid.

It's important not to underplay the time taken to build a community on a social media platform, which can be at the whim of social media companies that own the platform. In 2015, Facebook decided to prioritise Facebook groups (public or private forums set up by users with a common interest, as a hobby or physical location) over pages (usually an organisation's official presence on the platform). Many businesses that had already invested in gaining 'Likes' and followers on their page were going relatively unnoticed by users due to this change in prioritisation. A lot of these businesses then had to invest time and effort into creating new content for Facebook for more prominent advertising.

You can read Zuckerberg's announcement here: <https://www.facebook.com/notes/zuckerberg/changes-to-facebook-groups-and-pages/>

Implementation

It's important to test that the campaigns or a general online presence are working, and that the costs above have paid off – whether there has been an increase in sales, or website visits, or traffic to the company website. Targets may be placed, along with success criteria, to measure the effectiveness of the campaign.

For example, if an organisation kicks off a new marketing campaign via online channels, it should ensure that it is implemented following specific time frames. If the organisation offers a 'one get one free' offer via social media pages, it would be relatively easy to simply post the offer on social media channels. But the organisation should also ensure that any way by which the offer is made is up to date. This offer; for instance, customer service staff should be aware of the offer, and have customer phones or emails to place an order.

While many social media platforms are user-friendly and seem simple to use, testing is still important. Does the post appear as it should to an external user, or is a key part of the image missing on certain devices? Does the platform's algorithm or its promotion tools show the post to the right audience? If the business wants to track the success of the campaign, will tracking (such as using analytics) be possible on the different platforms?

**COPYRIGHT
PROTECTED**



Replacement or integration with current systems

In the modern world, businesses integrate or even replace older methods of work with new ones. For example, moving from paper to digital promotion – more relevant and cost-effective. The methods of work, the hardware, the software, the operating system, and any necessary software or accounts must be configured.

Productivity

Social media has the power to both help and hinder productivity. Replacing telephone calls with video conferences can help with productivity, or using online cloud services. However, staff could be distracted by social media during working hours.

Working practices

Businesses and customers have needed to find new ways of doing business and of providing services available through social media channels. Businesses need to check that their services are well-received, and to tweak them if they are underperforming.

Security

Social media is not a safe space. Some accounts are a target for hackers, some of whom may be able to damage a business or its reputation with its products or business tactics. This is a major problem and is especially a problem for smaller businesses which don't have a dedicated IT department, or accounts, or procedures in place for dealing with an incident. Hacking could be done by a hacking group, a rogue government or simply by a disgruntled employee.

Take a look online to find some examples of business accounts that have been hacked. Examples here: <https://immediatefuture.co.uk/blog/6-brand-damaging-social-media-hacks/>

Questions – C2 Online communities

1. Give two reasons why we must be careful when using social media.
2. What are the limitations of microblogs, or short videos such as TikTok?
3. How do chat rooms and forums differ?
4. How could social media damage a company's reputation?
5. Why are social media sites generally free to use (no monetary value to sites)?

**COPYRIGHT
PROTECTED**



④ D: Protecting data and information

In this chapter you will learn:

- ① The different threats to data – malware, hacking, phishing and accidental damage
- ① How to protect data and systems
- ① The role of legislation in protecting data and the consequences of (non-)compliance

D1 Threats to data, information and systems

Data is crucial to businesses – without it, a business could be out of business.

A business needs to protect its data from being stolen, lost or tampered with, because it needs accurate data to make crucial business decisions. There are many ways that data can be lost both accidentally and deliberately. This can include data on a local device, stored on a local server within the building, or stored on a cloud server or website or on the Internet.

Threats to data

Here is a rundown of some of the threats to our data and to business data.

Viruses and malware

A common form of data loss is due to a targeted malicious attack such as a virus outbreak, or **ransomware** attack. The files might be deleted, while encryption means that the files are unrecoverable without paying a fee.

If the fee is unaffordable, and there is no backup, the data is lost forever.

A particularly nasty virus could secretly destroy the files being backed up for several months. You might not notice until it is too late and most of its recent backup sets have been deleted. It's important to test that your backup system is working.

A disgruntled employee could also delete data. In some companies, IT staff might delete data at the moment that they hand in their notice; this eliminates the possibility of them damaging the system or to steal data. An employee could also plant a virus or logic bomb that activates after they leave.

Cyberattacks and theft of data are carried out by black-hat hackers. They are often carried out through software, through malicious downloads and booby-trapped adverts, or through phishing emails. The easiest way to defend against attacks is by using caution – ensuring that you have good security software installed, and being very careful when downloading files and viewing emails from unknown sources. Have the following tools at their disposal:

- **Malware** (malicious software) – there are the following forms, each with a specific purpose:
 - **Virus** – attached to a file, it spreads, thereby spreading the virus to other computers. When the file is opened – it may delete or overwrite files and cause the system to be corrupted, or steal data. Could be sent as an email attachment.
 - **Worm** – a program that self-replicates and opens many copies of itself, i.e. no need for a user to open it. A worm slows down the computer and network as it uses up the RAM and sends itself to other computers. Worms may have other malicious tasks too, such as rebooting machines or causing equipment failure. Worms could infect any vulnerable computer on a network by making use of software vulnerabilities and open ports.

Ransom
encryption
paid
decrypt

Malware
damages
ransom

Virus
executes
themself
and/or

Worm
that is
spread
and/or

INSPECTION COPY




COPYRIGHT
PROTECTED



- **Ransomware** – malware that encrypts some or all of the files on a computer. The user is given a cryptocurrency such as Bitcoin to decrypt the files. After a few days, the files become unavailable or the fee increases. However, if the user has a recent backup, they can just reformat the hard drive and load on the OS and files, avoiding the ransom.
- **Adware** – shows advertisements in order to make money for the creator (for example, through software, and often injected into a web browser).
- **Spyware** – software that 'spies' on the user. For example, it could steal login details to log in to your online bank. It could also inject fake adverts or pop-ups into the browser to redirect to other sites.
- **Trojan horse** – malware that pretends to function as a useful application, such as a fake antivirus product. Once installed by the user, it can deliver a viral payload such as deleting or corrupting data, or open up a backdoor so that more malware can be installed on the system.
- **Botnet** – a network of infected 'zombie' computers across the Internet that are listening for commands sent by the hacker to do things like perform Distributed Denial of Service (DDoS) attacks and out spam email, etc.

Hackers

There are three types of **hacker**:

-  **Black hats** – who hack maliciously for financial gain or to cause disruption (always illegal). These are the hackers that we tend to hear about on the news.
-  **Grey hats** – who hack into systems looking for bugs and report them to the owner (not necessarily malicious, but still illegal).
-  **White hats** (aka ethical hackers) – who are asked or paid to try to break into a system or product in order to find flaws and fixes before they can be exploited.

Some hackers start out as a black hat, and may later see the error of their ways and be recruited by a major cybersecurity company, or a government. Others only want to learn the skills legally.

You may remember that in 2017, the NHS was attacked by the ransomware WannaCrypt. A black hat hacker called Marcus Hutchins from Ilfracombe in Devon managed to stop the malware from registering a domain that the malware tried to connect to. At the time, he was working for a firm Kryptos Logic, who recruited him based on his blog posts, having started hacking as a hobby. He was a hero, but he was later arrested at the airport by the FBI in August 2017 while attending the hacker conference DEF CON. DEF CON is the world's most famous hacker conference, attended by law enforcement agencies such as the FBI. The arrest was made over concerns he had previously written, called Kronos. Over the next few months, he spent time in custody, but all charges dropped, and was eventually released in 2019, initially under close supervision.

Systems are attacked for a variety of reasons such as:

- **Fun/challenge** – sometimes the hackers don't intend to cause disruption or financial damage, but just want to see what they can do to a system they can gain. They may gain a reputation and kudos in the dark web community, however, starting this way could lead to darker activities, as was the case with Marcus Hutchins.
- **Industrial espionage** – attempts to steal valuable electronic property (intellectual property, secrets, formulas, plans and recipes. For example, hackers (who may have been recruited) stole trade secrets about the COVID-19 vaccine from companies such as Pfizer.
- **Financial gain** – hackers attempt to breach company and government servers to steal data to sell. A growing trend is to also infect a business with ransomware – data is retrieved from a backup or by paying the hacker the ransom, extorting money.
- **Personal attack** – for example, an attack on a previous employer by a disgruntled former employee, or an acquaintance or partner who they hold a grudge against.

**COPYRIGHT
PROTECTED**



Phishing

In the 1980s, hackers used to phone up IT departments or reception desks pretending to be employees at the company and asking for their passwords. Nowadays, passwords are much more secure and this tactic won't work.

But thieves and other malicious actors will still take advantage of human behaviour and people's mistakes in order to obtain information.

Phishing (fishing for information) attempts are emails, texts and phone calls pretending to be from someone or an organisation that the victim might be familiar with. Spear-phishing is highly personalised – the hacker has managed to find a few details about the victim. Some of these are very convincing as they look real and sophisticated due to the complexity of the scam. They are designed to get you to click on a malicious link, divulge your password or banking details, or to steal money.

Phishing – an attempt to get information about someone by making a phone call or sending an email with account details.

Here's an example of a phishing email subject line. If you had a NatWest account and clicked it.

Sender	Recipients	Subject
customersut@natifonline.com		We have tried to contact you about your account

But if we look carefully, the email should have come from the NatWest domain, natwest.co.uk, not natifonline.com.

It's not difficult to work out what the email would say if you opened it – it would take you to a page that looked like the real page so that you would type in your details. The hacker could then use to log in to the real site and attempt to take money from your account. There's a whole genre of YouTube videos called 'scam baiting' where people respond to phishing attempts and other scams – some of them are very, very sophisticated.

Here you can also see a text message received purporting to be from the Royal Mail. I'd have had a card pushed through my letter box had this been the case, and I'd have been asked to visit the Royal Mail website!

Accidental damage

People sometimes make mistakes and data is lost – for example, they might delete the wrong file, overwrite a newer version with an older one, cut text from a document without pasting it again somewhere else, or overtyping information by mistake. They might also throw away the only copy of information by accident, or by leaving a handwritten form or note, or by leaving a USB drive or laptop containing the only copy on a train. Data is permanently lost, not just a copy of it.

Accidental damage – may be caused by leaving a document or account open on a computer.

Hopefully, these are only minor (affecting single files or there are only a few lines to retype), or there is a recent backup or shadow copy or other technical measures in place to help prevent data loss, such as a digital recycle bin.

Large-scale data losses make the news – for example, if a government department accidentally deletes thousands of important records.

Sometimes the data loss occurs because of a hardware failure – a drive or even a corruption of magnetic storage media when in contact with a strong magnetic field, data, or someone could accidentally drop or knock over a drive or a computer with data on it.

COPYRIGHT
PROTECTED



Data can also be lost or corrupted by natural disasters, such as a flash flood, an earthquake, or a building fire. A burst pipe or a building fire can also be a cause. To prevent this, server farm protection built in (including no servers near the floor), and fire-suppression systems that don't damage electronic equipment.

Impact of threats, information and systems on individuals

Even the most wary of people fall victim to cyberattacks. One YouTuber (Jim Brown) consultant was temporarily tricked into deleting his own channel:

<https://www.youtube.com/watch?v=YIWV5fSaUB8>



Many people have been tricked out of money by online scams and phishing attempts that wouldn't work. An interesting channel that exposes scam artists is Pleasant Green:

<https://www.youtube.com/channel/UCAPrhJw7w0W445GzPoCISdw>

Falling victim to scams and phishing can lead to loss of money, potentially as devastating as the loss of financial loss and feeling of insecurity. Likewise a virus or ransomware could delete irreplaceable photos and other files – perhaps as upsetting as if a colleague died in a fire. Scammers often depend on the feelings of shame, guilt or embarrassment to prevent victims from reporting the crime as well. Finally there is the stress of dealing with phone calls to the bank and cancelling cards, etc.

Identity theft can be devastating to an individual. Can you imagine the stress you would feel if a credit card or mortgage in your name and you were expected to pay their bill? It can take a very long time and can affect your mental health. Your credit score could be affected, your ability to take out loans.

In the business world, scammers try to take on the identity of a real company to get money or pay for services, or to extort money from victims. These are called 'clone' scammers might send emails or set up a fake website pretending to be a bank, or a company. You should always check the company details thoroughly and report suspected clones (e.g. Action Fraud) or to a governing body for that industry (e.g. the Financial Conduct Authority relating to money).

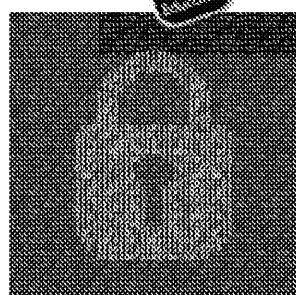
Impact of threats, information and systems on organisations

The impact on a business can be severe, especially if the company is fined millions for not protecting personal data about its customers and staff. Here is a quick rundown of the types of threats to organisations:

Data theft (data in transit and data at rest)

Data can be intercepted and stolen (unauthorised) when:

- It is being transferred across a network or through email. Unencrypted data can be intercepted, and weakly encrypted information can be unencrypted. However, if the traffic is now encrypted with strong encryption to keep the contents safe, even if intercepted, it cannot be read.
- If a drive or device is lost (such as a flash drive, a hard drive or a laptop), a hacker could access the data and/or competitors, and, in some cases, this could be a major security breach.



A system could be breached by an outside hacker directly or indirectly. An insider could steal or leak data or create a security breach. If data is leaked and sold on to others, there is no knowing how the data is held.

Data can be either copied, deleted or modified slightly. If a security intrusion may not be detected for months or even years, the security of the system.

**COPYRIGHT
PROTECTED**



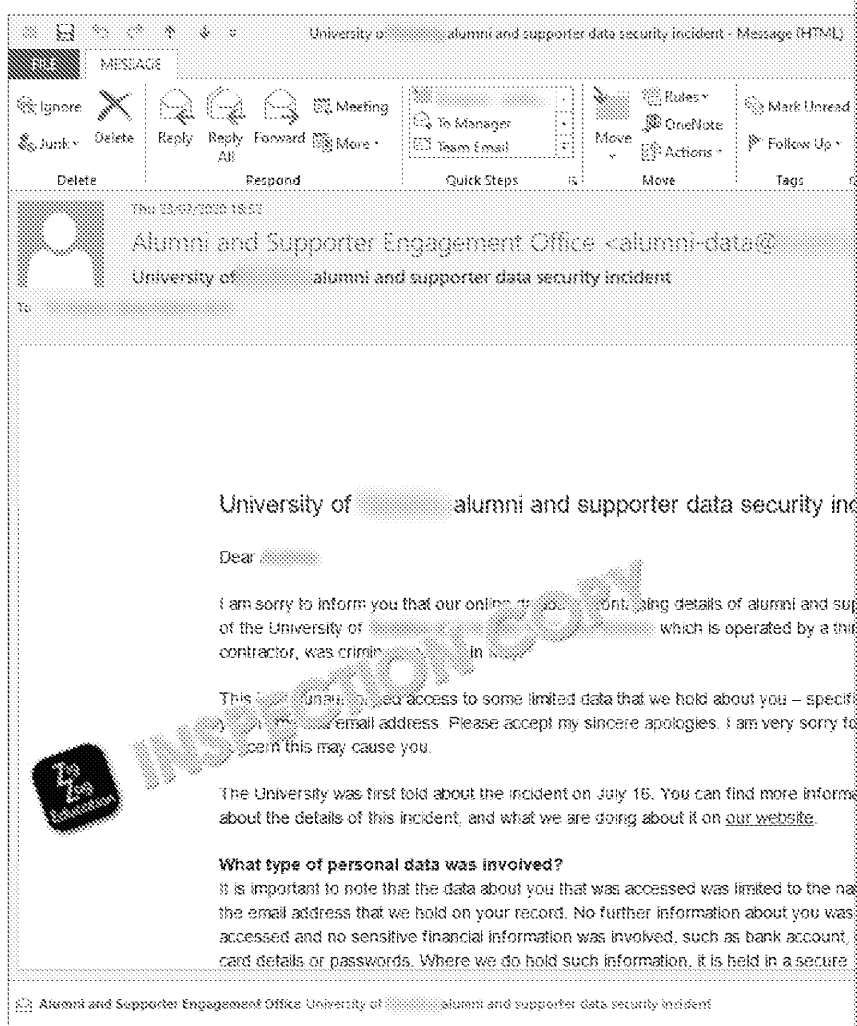
However the system is breached, there are many financial repercussions for the business may even be forced to close if it cannot financially recover.

In order to survive, businesses need a good plan to deal with an attack. The best first place by having good defensive measures in place. Don't think that it's just if attacked, although they're generally the ones you hear about in the news. Many medium-sized businesses because they've generally got the smallest budgets for experienced IT managers in charge, and may be forced to pay ransoms.

Data manipulation: there are so many ways that data could be edited by an attacker. For example, a company-owned or political website, or social media account, could be defaced by hackers (or 'hacktivists' – a play on 'activists') in order to slander the business or party. Such attacks are usually discovered quickly because of their public nature. Of course, a hacker or malicious insider could also alter data in a company-owned spreadsheet of accounts – these attacks might not be discovered for months. An employee could alter company financial data and poor business decisions could be made as a result.

Data modification is similar, but may be financially motivated for personal gain. alter their timesheet if there's a bug, allowing them to be paid extra, or an attacker could alter bank balances and move out the money.

Many universities and other organisations suffered from the Blackbaud data breach, millions of email addresses and other personal information.



Not a welcome email to receive!

**COPYRIGHT
PROTECTED**



Denial of service

Denial of service is exactly what it sounds like – denying (stopping) legitimate use of a service such as a website or server. Typically this is achieved by flooding a server with network connections so that the server's network connection becomes too busy to support legitimate users, or the server is overwhelmed by the amount of traffic directed to it. The amount of traffic directed to a server might be several terabits per second, sent from many different IP addresses controlled by the hacker (a botnet). However, you could also say that taking a system offline by a virus outbreak or worm, or encrypting data through a ransomware attack, is a denial of service. A denial of service can be taken offline by the IT admins while the attacks are being investigated and the system is being brought back online.

Denying a service is designed to cause financial damage to a business through:

- bringing down public platforms and lost sales opportunities
- reputational damage
- lost staff productivity if internal systems are disrupted

Denial of service attacks can be carried out by users or servers.

Denial of service attacks are often carried out at large corporations as punishment for the hackers' offence. Denial of service may also be political; an attempt to take down the system you oppose.

Denial of service attacks can be difficult to stop because all of the requests are sent from different IP addresses and it's difficult to know which requests are malicious.



Go to [zzed.uk/](https://www.zzed.uk/)

Take a look at some of the larger denial of service attacks that have taken place. A good starting point: <https://www.cloudflare.com/en-gb/learning/ddos/famous-ddos-attacks/>

Downtime is when a server might be taken offline by the attack, or might be switched off. If data is deleted, corrupted or modified, then the data has to be restored from backup. If data might be restored first, there could still be several days before all of the system is back online.

Loss of reputation

- **Public image** – when personal data is breached, the company may be required to inform their customers that their data was stolen. In large breaches for well-known companies, news of the breach is covered by national news channels and in newspapers and online news. Affected customers may lose trust in the company, and new potential customers might be put off from joining the company.

A good example is the telecoms company TalkTalk – its breach in 2015 made it clear that unencrypted details of 157,000 customers were stolen. Around 100,000 moved to other providers. TalkTalk still had millions of customers who stayed. The share price of TalkTalk fell significantly.

Loss of competitive advantage and financial loss

- **Competitive advantage** – companies which have suffered a large financial loss may lose their competitive edge over the competition. For example, they may lose customer loyalty or property.
- **Financial loss** – it was thought that the TalkTalk breach could have cost up to £100 million. Financial costs of a breach can include fines, forensic analysis, purchasing new systems, and loss of staff productivity and customers. In some cases the business may be temporarily closed and staff still need to be paid.
- **Reduced productivity** – if staff don't have access to servers, files, intranets and other systems, their job, they will have to work offline temporarily, possibly on paper or on a different system. Their work may take longer, and they have to manually add in the data once they are back online.
- **Legal action** – under the Data Protection Act 1998, companies could be fined for a breach. Under this act, TalkTalk was fined £400,000 for its data breach. In the UK, these fines are handled by the Information Commissioner's Office (ICO) – this was the largest fine that it had ever issued. See <https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/>

**COPYRIGHT
PROTECTED**



However, TalkTalk was probably lucky. Had the breach occurred a few years covered by the Data Protection Act 2018, which significantly upped the ante can be dished out. For the most serious breaches, there is now a maximum of 4% of global turnover from the previous year, whichever is greater.

In 2020, the ICO fined British Airways £20 million after the theft of details of passengers. The hotel chain Marriott International was fined £18.4 million as records were accessed six years previously, and occurred before Marriott even was responsible for the breach. The fines could have been a lot worse – they were £183 million for Marriott and £183 million for British Airways!

In August 2021, the online retail giant and web-hosting company Amazon was fined under GDPR. This is significantly larger than any other fine issued.

INSPECTION COPY

Question 1: Threats to data, information and systems

1. Identify two ways that worms and viruses differ.
2. Why are grey-hat hackers perhaps acting morally but their actions are still illegal?
3. While creating a new version of a spreadsheet recording sales for the year, you accidentally overwrites last year's sales instead of creating a copy and editing that. What is the potential for accidental damage?
4. A person is victim to identity theft and has a credit card taken out in their name. What problems that the person could face.
5. Explain why data theft is a problem for businesses.

COPYRIGHT
PROTECTED



D2 Protecting data

Processes and techniques for protecting data and systems

So we now know about the threats. While no system will be 100 % secure, there are methods that we can use to reduce the risks.

File permissions and access levels

Access can be restricted to computer system resources such as drives, files and printers. For example:

- Payroll and HR may be the only departments with access to salary and highly personal information (e.g. on a shared drive) – see the screenshot
- Only IT administrators may have access to company servers
- Only network administrators would be able to make substantial changes to the network infrastructure
- A regular employee might only be given read access to some shared drives
- System functions could be disabled entirely such as new software installations, access to the control panel or command prompt, etc.

These settings can be implemented in various ways. For example:

- Giving only certain staff admin accounts that allow them to access servers or more shared drives
- Selecting access to specific usernames only
- Setting appropriate file permissions (based on username or members of policy)
- Setting group policy on the server to automatically block certain activity

File permissions refer to security controls that a user can set to secure files from editing or formatting.

A file that can be shared and edited by more than one user is a read-write file, which can be accessed and read and can also have data written to it (for example, when the file is

You can change the attributes by making the file read-only. Selecting the read-only attribute prevents the file from being overwritten or amended. The file can be opened and read, but changes cannot be made to the existing file name. If you wanted to make changes to a read-only document you would need to create a new file from the read-only check box.

Backup and recovery procedures

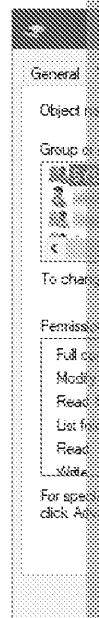
We need to keep copies of our important data in case the original copy is lost or corrupted. Backup is the process of copying those files to external storage media.

Most companies will back up their most important data every day, some even several times a day. Without data, the company wouldn't be able to function effectively and could even close.

We can back up:

- an individual PC or Mac using a backup utility built into Windows or macOS or a third party tool
- a server or many servers at once using built-in server backup utility or third party software
- remote machines are copied across the network
- a single file or folder, or the whole machine

File permissions
group permissions
examining permissions
may be different
Access levels
copy permissions
they can be different



INSPECTION COPY

COPYRIGHT
PROTECTED



Backup procedures
follow the order of importance

Recovery procedures
follow the order of importance

There are several types of backup that are used:

A **full backup** includes all files that are to be backed up. This takes the longest to run and takes up the most storage space. A full backup might include all of the following:

- User profiles and user data
- Shared drives and shares
- Databases (customer, sales, etc.)
- Email databases

You may hear the term 'system image' backup. This is an exact clone of a hard drive, which includes the operating system, applications and all data. Restoring this backup will restore the device back to the exact state.

An **incremental backup** backs up only the files and folders that have been modified since the last backup (either a full backup if this is the first incremental backup, or since the last incremental backup). Incremental backups are the fastest to create because only the data that's changed is backed up. To restore, the first full backup must be restored, and then each incremental backup in order that the files are created.

A **differential backup** is slightly different. Like an incremental backup, a full backup is performed first. A differential backup copies all of the data that has changed or was created since the last full backup (or since the last differential backup). So if a full backup was performed on Monday, Tuesday's backup would include Tuesday's files. Wednesday's would include both Tuesday's and Monday's files. The backup time will increase each day, but restoration is faster than incremental. Only the latest differential backup is required following the full backup restoration.

Disaster recovery policies enable a business to recover quickly after its servers have suffered from the following:

- a cyberattack, such as data deletion or modification, or a ransomware attack
- physical theft of drives or servers
- a fire in the building that has destroyed the server
- a flood or other natural disaster
- hardware failure, e.g. too many failed drives or a failed server
- data corruption
- accidental deletion by a member of staff
- power cuts – in the UK it is very rare to lose power for more than a few hours, but businesses can occasionally experience a day or more without power (e.g. Texas in 2021)

If the data is hosted in the cloud, the owner of the remote server will be responsible for the disaster management plan. The IT department in a business that uses on-premise servers is responsible for maintaining and implementing the plan.

The plan will rely on data being restored from backup media. Backups are usually sent to another server once or twice a day, or to tape/disk. Some systems even insert tape automatically.

At least one backup is kept off-site in case the whole site is destroyed. The more often backups are taken, the less data is lost. The faster the business gets up and running again, the less of long-term damage.

Components of the plan include:

- the frequency and storage location of backups
- the physical and logical security of the system
- who is responsible for updating and implementing the plan
- the actions that staff should take after a disaster to get the data restored again

**COPYRIGHT
PROTECTED**



Of course, a disaster recovery policy is never idle or forgotten about, gathering details and remain up to date at all times with updated job roles (rather than staff names being replaced over time), and include any new risks, mitigations and updates. The procedure for occurrence. Regular testing of the backup system is necessary.

The disaster recovery policy will include:

- What everyone will be doing to ensure that no steps are missed, the work is done, and don't perform the same task.
- What staff should and shouldn't do – everyone in the company might be involved in the plan on paper temporarily and not reporting news of a breach to the media.
- Who is responsible for making sure that the backup is running successfully, reporting when and how data is backed up, which drives or tapes are used, off-site storage.
- Timeline for disaster recovery – which data and equipment will be restored first, the infrastructure needed by the company for it to run successfully), and which is the last.
- What will need to be done if the office location needs to move either permanently or temporarily. If the office is destroyed in a fire or becomes uninhabitable due to the pollution, specify what network infrastructure, servers, hardware and software is needed, purchased for the move, and how the data will be restored at the new location. Also cover the loss of staff, for example, if the office is located in a hazardous area.

It is often stated that 60 % of small and medium-sized companies that are attacked go bankrupt within six months of being hacked. They are often targeted by hackers because they lack the expertise to protect themselves. There are probably a number of reasons for this:

1. Limited cash flow – and are bankrupted by fines and may not have been in a good position to recover.
2. Lack of backups, or non-working, untested backups.
3. Loss of files and databases crucial to the functioning of the business.
4. Loss of reputation and customers.

Passwords

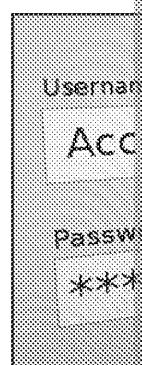
We use **passwords** to log in to websites, services such as email, and devices. A password is a string of letters, numbers and special characters. Passwords are often not particularly secure because we're terrible at remembering strong passwords.

*OleY 2DXR*1Ed)2r%gWo* is a very strong password – it's long, and it contains a mix of letters, numbers and symbols. It would take a computer billions of years to try different combinations. The problem is that it's terribly tricky to remember. In fact, you are trying to remember 20 or 30 such passwords. So, people often use simpler passwords. The most common passwords include, and I'm not joking, 123456, password, 11111111, qwerty, abc123, and password1. If you use any of these, go and change them now! Some experts think that the length of a password is more important than its complexity.

When you sign up to sites, there are typically requirements such as setting a password containing a minimum of eight characters. Even so, many people use the same password across many different services because it's easy to remember. This is a bad idea. If your password is leaked, they can find your email address, and you've used the same password, then they have access to your email. If they can just use password resets to lock you out of any services that don't use two-factor authentication.

Password

letters, numbers, and special characters to authenticate a user or service into a system.



**COPYRIGHT
PROTECTED**



People also recycle passwords – they simply add another number to the end. So 'password1' becomes 'password2' or 'password12', but if someone found your original password, that's not much help. You should also regularly change your passwords as an added precaution, just in case you've already logged in to your account.

The more secure a system, the more frequently users are required to change it – every three months, or every year.

You should never write down your passwords or store them in a document on your desktop. The best solution is to use a password manager that you set one long password for – that software will store all of your passwords in an encrypted file, and you can enter those passwords into sites and services.

You could make up a mnemonic to remember a long password, e.g. 'When I was in London, it was great!' would become 'WILG!m#63PDL,iwgl!'. According to <https://www.kitfox.com/PasswordStrength/> it would take about 300 million years for that password to be cracked. Needless to say, guessing the password is a lot easier.

Some documents are confidential or contain sensitive information which should only be accessed by authorised users. Document passwords are added to make sure that unauthorised users cannot access the information.

When a character is typed in it is displayed as a * or •. This is to ensure the privacy of the information.

Physical access control

You have probably seen in feature films that employees in some companies or government agencies carry access cards that can be used to access specific parts of a building (usually with a villain attempting to access the parts that they shouldn't). This is true of many organisations – only a few trusted IT staff will have access to the server room, while a regular employee might only be given the code to the front door. They may have a card that allows them to enter the building only during their contracted hours, and new starters may not be given the door code for several months until they are trusted.

You may find this when you go to college or university – for example, your access card may only work to enter your department building, specific libraries, or your own hall of residence. If you have access, your card may only work until, say, 6pm.

We can use traditional locks and metal keys, swipe cards and **biometric** locks (which use your iris) to:

- physically lock the room where data is stored (e.g. the server room)
- secure access to the building (including windows), especially overnight when no one is there.

Highly secure facilities, such as data centres, have very few external doors. They are unlikely to have windows, which can be weak points in the building's security. Shutters may also be used at night.

We can also lock down computers and devices. For example, laptops, tablets and computers can be locked to a desk or immovable object, or placed inside a cage and secured with a tough metal cable. When locked down, the mechanism to open the cases of desktop computers is also disabled, meaning that hard drives cannot be removed. When travelling, always keep your person or within sight, and use a plain-looking bag, such as a rucksack with a lock, rather than a fancy-looking laptop bag. This may deter thieves.

**COPYRIGHT
PROTECTED**




Many devices such as laptops and phones also have a fingerprint sensor built in or a home button. You might be able to use a camera to log in using facial recognition, or scan a unique pattern of your voice for verification.

Some systems use **two-factor authentication** – a combination of a password and a smart card or key generator. This adds security if the device is stolen, as both the password and the card or key generator (a physical token) must also be obtained.

Keys and swipe cards or smart cards can be stolen or borrowed. Biometric security can be more secure, but some older systems could be hacked with a detailed photograph (modern systems have removed this limitation as the points are viewed from multiple angles). There are also privacy concerns over companies storing personal data such as a fingerprint. Some people may not want to be identified by a person if they choose to alter their appearance, and voice recognition may not work if their voice changes.

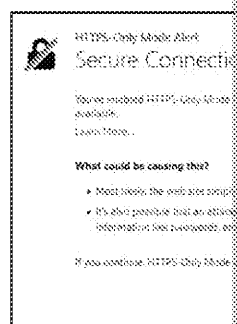
Digital certificates

Digital certificates have a unique key within computer systems and networks. They are used to verify the identity of a website or person – preventing man-in-the-middle attacks. If you see a warning that a site is not secure, it means the certificate is invalid (if it has expired or doesn't exist), or you will get a warning that the site might be unsafe. In January 2019, many websites owned by the US government were inaccessible because a government shutdown meant that expired certificates couldn't be renewed – even the NASA website was unavailable without attempting to bypass security checks.

You are probably most familiar with the certificates used to verify the owner of a website. You will find one associated with any website that uses HTTPS. You can view them by clicking on the padlock icon, like this . They used to be green, but now they are grey or black because they are pretty much expected.

Some browsers, such as Firefox, will warn you if you are not using HTTPS (no certificate). You may have to turn this feature on.

Digital certificates are used to verify the identity of a website or person – preventing man-in-the-middle attacks.



If you run your own server, you need a certificate. Because anyone can get a certificate, they're not trusted. You'll get a warning (like this screenshot) if you want to access the site. Click the 'Advanced' button and 'Proceed anyway'.

The most trusted certificates are issued by a Certificate Authority (CA). Certificate authorities such as IdenTrust, GoDaddy, DigiCert, GlobalSign require a fee to generate each certificate, and they expire after a while, perhaps

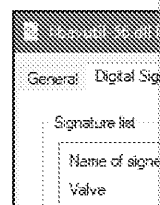
**COPYRIGHT
PROTECTED**



You can take a look at the fees here: <https://www.techradar.com/uk/news/best-free-ssl-certificates>. Fees vary wildly between each provider. Let's Encrypt is a free service, but the certificates are only valid for 90 days. Take a look at some different certificates – here is the one for the BBC. We can see the company, the validity period, the issuer of the certificate and the sites that are covered. These details are provided to the CA in order to verify the company and generate the certificate.



You will see certificates or digital signing in other places too, such as driver and file signing within the Windows operating system. Here's an example of a file used by the application called Steam, produced by the company Valve. Digital signatures are also required when installing printers and other hardware. Documents can also be digitally signed, instead of signing a printed copy.



Protocols

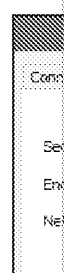
We've already discussed what a protocol is (the rules for communication), and we'll now go further and discuss how HTTPS works.

We've got a clue by looking at the detail of the BBC's certificate:

Technical Details

Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3)

Specifically, we're looking at **Transport Layer Security** (TLS). An older standard is SSL. TLS is used by the majority of sites. These protocols use encryption to scramble and unscramble the data, and a public and private key is generated (more on that later). The web browser requests the TLS or SSL connection from the web server. The server responds by issuing the certificate (which is the part you can view) and based on the encryption key sharing, the connection is secured. Your web browser will check that the certificate is valid – which is why all of those government sites were inaccessible in January 2019.



COPYRIGHT
PROTECTED



In addition, we encrypt our connection to the wireless router. In a home or small business (WPA = Wi-Fi Protected Access). You should be familiar with this set-up – every device on the network uses the same password and is verified by the router. In larger business environments, each user has a unique password to connect, and the authentication is handled by a separate server. This makes the network much more secure.

An older and now very insecure protocol is WEP (Wired Equivalent Privacy), which is no longer recommended.

You may have noticed 'AES' in some of the screenshots – this is just the type of encryption (Advanced Encryption Standard). You may also see the older RSA encryption still in use (named after its inventors: Ron Rivest, Adi Shamir and Leonard Adleman).

Using antivirus

Antivirus software stops the download, installation and running of viruses and other malware, including spyware and, more recently, ransomware. Some antivirus software also detects malware that is already installed on your system, through regular scans and constant monitoring.

In the past, this could slow down a computer, but nowadays the performance drop is minimal.

Antivirus – software that scans incoming files and applications, and when the need arises quarantines and cleans up viruses that aim to harm your system



Antivirus does this by looking for the characteristics of the files, their behaviour and processes on the system against a set of known malware signatures. If a file is infected, it may attempt to remove the infection (disinfect), delete the file, or stop it from running, placing it in a protected 'quarantine' area. Antivirus software is essential for laptops and smartphones, and is recommended for smartphones and tablets.

This means that the antivirus must constantly update its definition of known threats. Most manufacturers update their definitions by downloading the files from the server several times a day; for example, Symantec, Sophos and Microsoft. Each time a new malware sample is provided, a new definition is made. Because this set of definitions can be very large, some antivirus software requires an active Internet connection when running for best results. It can make checks against a cloud database as the downloaded version might contain only common and recent definitions.

But as there are thousands of new malwares created each day, there is often a delay in updates. Therefore, antivirus software tries to detect unknown threats based on suspicious behaviour, such as file replication or high CPU usage.

Antivirus is often preinstalled with the operating system (Microsoft Defender), and some are free (e.g. Avast and AVG) or paid for (e.g. Norton, McAfee and Sophos). Paid-for versions often require a subscription fee for the product to keep working and/or receive updates.



**COPYRIGHT
PROTECTED**



Using firewalls

A **firewall** simply allows some network traffic to pass through, but blocks other traffic. This allows us to specify which traffic is legitimate, and helps block hackers from gaining access to the system by blocking the ports (doors) that can be exploited. We determine what traffic is allowed to pass through and which is blocked using a series of 'rules' certain ports, IP addresses and domains, etc. Firewalls usually come with common admins can change (configure) these rules to meet the needs of the business.

Firewall
security
network

Firewalls nearly always filter incoming traffic – this is to help prevent hackers from accessing the internal network. Some, but not all, filter outgoing traffic generated within the internal network. This is useful because the firewall can sometimes be used to stop a malware program from 'phoning home', or uploading files to a remote hacker. Firewalls that filter both incoming and outgoing traffic are 'two-way' firewalls.

There are two types of firewall:

1. **Hardware firewall** – a physical device that plugs into the entrance of the network between the public Internet and the private LAN. All network traffic passes through the network infrastructure is located behind it. Hardware firewalls can be controlled via a web interface. They are expensive and purchased with several years' worth of support. After several years, the device may no longer be supported and the hardware, sometimes with an upgrade discount.
2. **Software firewall** – this can either be built into the operating system, be part of a security suite, or be a stand-alone application. The software firewall is a second line of defense, but it also helps to prevent a compromised computer on the internal network from spreading malware across the system.

A proxy server can be used to achieve a similar effect.

Methods of encryption

Encryption is where normal text (plaintext) is converted to cipher text using an algorithm and one or more 'keys' which are often very long numbers. This means that if an encrypted file is intercepted, then it is very hard to read it without the key(s) needed to decrypt it. Using two keys (asymmetric or end-to-end) encryption is much more secure than using one key (symmetric) encryption.

This makes it very hard – often impossible – to unscramble or 'decrypt' the data without the correct key(s) as millions of combinations of numbers must be used in order to decrypt the data. The longer the keys, the harder it is to decrypt an intercepted file.

A system that uses **two different keys** (asymmetric) is more secure than a system that uses **one key (symmetric)** to both encrypt and decrypt because it's easier to decrypt with a single key.

Symmetric encryption uses one secret key that may only be used once. The key might be 128 bits or 256 bits. It is used to send large quantities of data. It's fast to encrypt and decrypt, but it's not a particularly secure method.

Asymmetric encryption uses a public key and a private key. The keys are both prime numbers that are multiplied in order to encrypt the data. The private key (one of the prime numbers) is used to decrypt it, and is used by the recipient for that purpose. Secret keys can be exchanged through asymmetric encryption. Because the numbers are larger, the process is slower and requires more processing power, but this is essential for the safe transmission of data.

**COPYRIGHT
PROTECTED**



Stored data (data at rest)

We can encrypt individual files, databases and whole drives using a password or key. This is useful when taking data off-site – a lost USB flash drive is less of a problem if it's strong. We should always encrypt sensitive data and password files – theft of unencrypted data or drives can constitute a major data breach and large fines can be imposed.

In Windows, drives can be encrypted using BitLocker. Individual files can be encrypted (e.g. in a file system), and individual applications such as Word and Adobe Acrobat can set passwords.

Data during transmission

We can also encrypt data as it is sent across a network and the Internet using encryption keys. This means that if somebody intercepts the data (e.g. a man-in-the-middle attack), it is harder for them to read the content. We use a lot of different methods of encrypting data. For example:

- Set Wi-Fi passwords that encrypt the connection to the router
- Use HTTPS when sending data across the Internet (including online banking, shopping, email, and social media) – look for the padlock icon in the browser address bar and some browsers can be set to warn you when a site only uses HTTP. Browsers used to display green padlocks and bars, but have since removed the green because it's now so normal to use HTTPS.
- Use VPNs to form an encrypted network tunnel across public networks
- Use encrypted communication platforms such as WhatsApp and Signal
- Use apps that encrypt all of their network traffic
- Email is also encrypted when it is sent (e.g. using TLS)

You might think of encryption as being a modern invention – not so! Take a look at Bletchley Park during World War II in breaking German codes.

Current legislation for protecting IT systems

The main legislation that affects the UK is the Data Protection Act 2018 and GDPR (General Data Protection Regulation). We'll cover these in depth later in this companion.

All businesses that handle personal data (names, contact details, and other personal information and history) must comply with the spirit of the legislation. If they don't, and data is breached, they can face fines.

The impact of legislation on individuals and organisations

There are lots of methods that businesses should or could use to comply with the legislation.

On a personal level, you now have more control over your data, can request a copy of your data, and request that the company updates or deletes data about you.

From a business perspective, compliance can be expensive (but not as expensive as not complying). Companies with more than 250 employees must register with the Information Commissioner's Office (ICO) and appoint someone or collectively take ownership within the company to control how data is handled. For smaller businesses and large data-processing organisations, a specific data protection officer is required.

These appointments cost money, as do the creation and implementation of plans, and the purchase of software – antivirus, firewall and anti-spam subscriptions, and upgrading to newer, supported software.

Other requirements could increase administrative work, such as fulfilling information requests from 'data subjects', whom the data is about such as you and me, or ensuring that all of the data is stored within the European Union, etc.

**COPYRIGHT
PROTECTED**



Codes of practice from the Information Commissioner's Office

Each IT system is unique, so there's not a single cover-all practice to comply with. You must use the guidance and follow it in spirit. But the exact wording of legislation can't be ignored.

Codes of best practice are published by the **ICO** (a public body that ensures that information rights are maintained) that sets out the sorts of things that companies need to do in order to be compliant, with guidance on specific subjects such as marketing. Since the IT systems and types and use of personal data are broadly specific to each industry, the trade associations sometimes publish their own codes of practice (with sign-off from the ICO). For more information about the ICO, go to <https://ico.org.uk>

ICO – Information Commissioner's Office
The body in the UK responsible for ensuring that organisations follow the data protection laws. For example, businesses that process personal data must immediately notify the ICO if they have a data breach.

Industries will often have a professional body associated with them, which helps to set standards and provide a source of news and information, uphold standards and the accreditation of members. Some of these bodies also audit the profession, or inspect the business to ensure that standards are being maintained. So joining a professional body raises the performance of both the individual and the industry as a whole.

In the IT industry, a professional body is the British Computer Society (BCS), which provides a source of news and information, upholds standards and the accreditation of members. If you're interested, take a look at <https://www.bcs.org/policy-and-influence/> and [qualified/certifications-for-professionals/](https://www.bcs.org/qualified/certifications-for-professionals/). An IT professional can become a member (the 2021 price is £120 per year). You can also take a look at their bookshop to see some of the books they sell (<https://shop.bcs.org/store/221>).

Questions – D2 Protecting data

1. Explain why a business will restrict access to data between staff in other departments.
2. What is the role of backup within a disaster recovery policy?
3. Why does adding physical tokens, such as a key generator, make digital authentication more secure?
4. Why are firewalls used within business-grade IT systems?
5. What are the advantages of using asymmetric encryption over symmetric encryption?

**COPYRIGHT
PROTECTED**



⑤ E: Impact of IT systems

In this chapter you will learn:

- ① How individuals and businesses use IT systems and are impacted by them
- ① How we source, verify, process and interpret data

E1 Online services

Using online services is now a big part of the everyday lives of many people.

Using online services in:

Retail

Online shopping has really taken off since its development in the 1990s. Amazon, for example, started in 1994 as an online bookseller and has become the biggest online retailer in the world, selling just about everything. In 1994, not many of us even had Internet access in our homes. In 2020, \$197.3 billion passed through Amazon's online stores. This doesn't cover the huge sums that Amazon took in from its online web hosting service, Amazon video streaming (Prime Video), smart speaker market (Alexa) and eBooks platform.

Nowadays, most physical stores include an online counterpart in order to stay competitive for a lot of customers who can order online 24/7/365 at a time that suits them. It's because it's cheaper to operate warehouses than high-street stores, and shopping bricks-and-mortar stores are closed. With online shopping, orders can be sent out via courier and parcel delivery services, click and collect from the closest participating local delivery depot, convenience store, Argos (for eBay) or other participating stores.

In 2020 and 2021, we learned to rely even more on online shopping during periods when shops were closed by the government, people chose not to go to the shops to reduce the risk of people testing positive for COVID were forced to self-isolate and, therefore, were not allowed to leave their homes. Food delivery slots from supermarkets were snapped up weeks in advance for the first time ever, and that trend is likely to stay in place for the time being.

Online selling platforms are also set up for third-party use; for example, businesses can create an account with eBay and pay listing fees, along with a percentage of the final sales price of their own goods, and can set up an online shopfront, allowing customers to see what they have for sale. eBay is a very general selling platform, but specialist platforms are also available for books, AbeBooks, and music, e.g. Discogs. Some people have even started entire businesses buying up pallets of returned items, selling items bought at charity



Many of these selling platforms are also open for individuals to list and sell items. These are called C2C (**consumer to consumer**) sales. In this case, the sellers and items are located in private homes. The seller is responsible for packaging (to the highest standard) and must organise to drop off the item at the courier's depot, shop / post office counter. Some sellers sell from their homes; for heavy or bulky items, a collection service is an option.

This type of selling is common through eBay and Facebook Marketplace. Many people also sell collectables through Etsy, as well as list items on specialist sites.

INSPECTION COPY

COPYRIGHT
PROTECTED



Some well-known high-street stores have closed in recent years due to the high online presence. In 2021, the chain of department stores Debenhams was bought by a private company and the stores and used the Debenhams brand online, largely to promote Boohoo goods. A physical store will need to exist because some suppliers are hesitant about supplying to an online-only establishment.

Financial services

Just as shops started to close down, banks also closed. I recently saw news that in over six years, 200 towns and villages had only one remaining bank. Not everyone has access to online services, or can travel to the nearest branch. Others prefer cash; for example, to buy a house.

Nowadays, most banking can be done online or through a smartphone app. It's easy to transfer money, arrange overdrafts and pay others: all online. Monzo, for example, was set up in 2015. Online services such as PayPal allow easy money transfers between accounts. It's even possible to apply for a mortgage online – probably the biggest investment of most people's lives.

Other investments can also be made online, such as buying and selling shares on the stock exchange. You can also invest in Premium Bonds online. If you are a Premium Bonds holder, you are automatically entered into a monthly prize draw whereby a computer called ERNIE (Electronic Random Number Indicator Equipment) randomly selects the prizewinning numbers of Premium Bonds. (You can see several iterations of ERNIE over the past 60+ years!)

Education and training

Following the coronavirus pandemic, you should be experts in the use of online education systems! Here are just a few examples:


- Virtual learning environments (VLEs) – online teaching resources and document downloads, quizzes, coursework submission, online work feedback, etc.
- Online revision platforms, such as ZigZag Education's eRevision platform – <https://erevision.uk/>
- Online video courses, e.g. <https://www.pluralsight.com/>
- Online exams (some new GCSE packages, and professional qualifications such as the CIMA exams at home instead of taking the exam at a test centre)
- Open University courses (usually paid for, with some free OpenLearn modules) – <https://www.open.edu/openlearn/>
- MOOCs – Massive Open Online Courses, which are free – <https://www.mooclist.com/>



News and information

Print newspapers have been in decline for many years because of digital offerings. During April 2020, print sales for some of the UK's leading national newspapers fell by up to 39 % due to the start of the coronavirus pandemic and the first lockdown – people went shopping less frequently and were not reading papers purchased by organisations like schools and libraries.

<https://www.bbc.com/media/2020/may/21/uk-national-newspaper-print-sales-plunged-coronavirus-lockdown>

 Go to [zzed.uk/115](https://www.zzed.uk/115)

Many news sites such as BBC News and *Metro* have always been free (the BBC used to offer a news service on Ceefax, its teletext information service). You can sign in to receive personalised news. All of the papers have a website – some are free, such as the *Guardian*, others, such as *The Times*, require a subscription to access, or allow only a few free articles, called a 'paywall'. *The Sun* temporarily introduced a paywall in 2013 but removed it in 2014. The free *Daily Mail*.

**COPYRIGHT
PROTECTED**



News channels are now broadcast online, such as BBC News 24 Live, and Sky News on YouTube. The main news channels also upload clips to news sites. Major news channels report on events, such as government press conferences, that include links to Twitter and other social media sources (although this can lead to 'bubbles' and sharing of fake news, or biased information).

News is also uploaded to social media sites such as Facebook by news companies and individuals. Articles are shared by friends.

Entertainment and leisure

This is a very broad category! We could include video-sharing sites such as YouTube, catch-up TV channels, streaming services, podcasts and music streaming, such as Spotify.

Entertainment could also include downloading games and playing multiplayer games online from Steam or other online services, or through the online stores of different games companies such as Sony and Microsoft. Entertainment apps can be downloaded on smartphones and tablets. Some support both in-person and remote play, and many board games are available online.

However, online gaming can be addictive and expensive (as can online gambling). Purchases to buy upgrades, downloadable content, and loot boxes have increased in recent years because some people see them as a form of gambling by paying money for a chance of winning prizes. Children have also racked up large fees on their parents' credit cards – it's hard to visualise them as real money, especially if they have a points value.

Productivity

Again, there is a wide range of online productivity apps for many different devices. Productivity applications such as Office 365 and Google Docs to VoIP applications such as Teams and Zoom, and tools and instant messaging such as Slack, and apps that support remote working. The tools on the modern workplace are discussed in the next section.

Booking systems

Nowadays most things can be booked online rather than over the phone or in person. This includes transport (trains, buses, aeroplanes, etc.), entertainment such as cinemas and events, tourist attractions and theme parks (sometimes cheaper online so that the staffing requirements can be known in advance). Holiday and hotel bookings are also commonly made online, as are restaurant bookings (shown) and services.

Some bookings generate a reference number or barcode that can be shown directly on a smartphone, or printed or written down. Some turnstiles at the entrances to attractions have barcode readers that can read directly from your smartphone. A separate app is required to generate the booking and collect the payment, such as the one shown.

Online booking can be much easier and quicker than booking on the phone, is available 24/7 (fewer staff costs). However, those without access to the Internet cannot use the service and could end up paying more.



**COPYRIGHT
PROTECTED**



Uses and implications of:

Transactional data

Every time you make a purchase either online or in store, in a coffee shop, etc., you generate **transactional data**. This includes the date and time, the store number, the cashier number, the items you've purchased, the payment method, and so on.

Transactional data – information generated when goods are sold either at the till or online with details about the product, price, credit/debit card number, customer details, etc.



While this data may not be particularly useful to you, it's crucial for the retailers. On the short-term basis, they need to know their stock levels so they can order more stock if necessary. But supermarkets and retailers run into billions of transactions. They can analyse this data to find which products are and sales of products vary throughout the year. By combining this with weather data, if the temperature outside reaches 25 °C – BBQs, paddling pools, salad items, etc. to ensure a successful summer? If Easter is warm and sunny, how many people will

Your parents (or you!) may have loyalty cards for various supermarkets. A loyalty card track everything that your household eats. Based on tracking your purchases, they know you've got children, if you're vegetarian or vegan, if you have allergies, when you have how many people are in your household. They can send you money-off vouchers for things you buy, or think that you might like, to try to keep you a loyal customer.

Remember that transactional data isn't just about retail. It's generated when you use your library account to view a magazine online, claim on your insurance, pay off a loan, or between bank accounts, etc. Businesses also generate transactional data internally.

Targeted marketing

Targeted marketing is the sending of promotional material to a specific demographic such as a specific age group or sex, or those who might be interested in purchasing the product. They might have purchased something similar from the company before, or have cookies on their computer (you may have noticed that things you look at on online stores can follow you around the Web).

Targeted marketing – promotion of goods to specific people, e.g. based on their previous spending, loyalty cards, etc. or demographic

Here are a couple of examples of targeted marketing:

Email marketing works exactly as it sounds – email sent to existing customers to sell new products, services and events. Generally, the emails are sent as HTML format, allowing for attractive formatting including fonts, layout and images, often set up in frames. They often contain an image or a pixel that can be used to track whether the emails have been opened, helping senders work out how effective the marketing campaign has been (based on the number of sales). For this reason, some email clients such as Outlook automatically block images.

Email marketing can be very cheap (compared to postal marketing, for instance), reaching thousands of recipients at once. Businesses can either send out the email from their own accounts with mailing companies such as MailChimp, SendGrid and other providers, or have the chance of the emails being flagged as spam by the recipient's email provider.

Businesses need to set up their mailing lists based on customer opt-ins and curate the list by removing expired addresses and honouring unsubscribe requests. The biggest shake-up to email marketing requirements, which are discussed later.

**COPYRIGHT
PROTECTED**



Social media adverts are displayed within the newsfeed of users of sites such as Facebook and Twitter (celebrities (governments, even). Social media can deliver highly targeted ads based on your location, status and what you've interacted with (commented on, liked, visited, etc.). The ads are often very effective. During 2020–2021, the UK government targeted social media users with messages concerning social distancing and vaccination.

There are many other forms of advertising, such as paper-based and telephone. A large number of non-addressed flyers and brochures appear on the doormat (and in the paper recycling bin).

Website advertising – many websites partially or fully fund themselves through advertising by other companies. They often make use of cookies, the small text files stored on your device by websites – that's why you often see adverts for the items you've looked at or visited. They are delivered as banners across the page or down the sides. The most obnoxious ads are those that hover over the main text, or sometimes take up the page entirely until you remove them. As many people use browser extensions called ad blockers to stop the adverts displaying, some sites refuse to work until you have disabled the ad blocker for that browser. This is common for adverts on traditional-style and local news sites.

Adverts also play before and during many online videos, including YouTube – a platform that monetise their work. You can often skip these adverts after a few seconds, depending on the video. Sometimes these adverts are fairly specific to the genre of the video.

When you visit a website, a small text file called a cookie is sometimes stored on your device as part of an automatic process, but now because of privacy concerns (in EU and UK law sites must ask you to confirm that you are happy for them to be stored on your device.

Our site uses cookies. Some of the cookies we use are essential for parts of the site to operate and have already been set on your device. To find out more about cookies on this website, see our [cookie policy](#).

Some cookies are very useful or are needed for core functionality of the site. Cookies allow you to access recently viewed items again quickly, and keep the items in your shopping basket.

However, cookies are usually stored in plain text and can be read by other websites. Some advertising services to see which sites you've visited and show you adverts related to what you've probably noticed that things that you've looked at on shopping websites appear in other places.

You can take a look at which cookies are stored on your computer. You can set your browser to not accept cookies automatically if you're concerned over your privacy. Some antivirus software might also block cookies, especially the ones that can be used to track your online activity.

Collaborative working

Many companies have embraced online technologies, which allows for the following:

- **World teams**
 - Members of the team are located in different countries
 - This allows recruitment from a much larger talent pool
 - Multinational companies can share resources and workload between their offices
 - A diverse workforce allows for a rich melting pot of ideas and creativity, making products more innovative
- **Multiculturalism**
 - Teams include a wide range of backgrounds, cultures and religions
 - Barriers are broken down between race, gender, age, etc.
 - Very insightful, allowing the team first-hand experience of launching products across different markets – they know what is accepted and what is taboo across different cultures, how the product could be tailored to different markets, allowing the right products to be delivered in the right places

**COPYRIGHT
PROTECTED**



- **Inclusivity**

- Modern tools such as methods of input into computers and the use of screen readers can help people use and access the technologies if they have disabilities

- **24/7/365**

- By having access to teams around the world, the different time zones can be used to provide a much longer service, which is an advantage. For example:
 - Customer service and online support chat can be carried out in different areas of the world to maintain 24/7 support – helped by the Internet and cheap global telecommunication. Countries that don't celebrate UK bank holidays or public holidays are able to carry on receiving calls if a UK contact centre is closed for the day.
 - Projects can be completed more quickly if one team finishes for the day and the next country is able to pick up where they left off – modern communication tools allow to leave messages for the next one
 - Allows staff to work more flexible working hours
 - Ordering and order forms are available for customers to purchase goods even when the shop is closed

- **Flexibility**

- Much greater flexibility for off-site and on-site work, and hot-desking, casual, temporary and permanent staff. A laptop and VPN set-up would allow staff to work in shared meeting rooms, or work at other sites and offices temporarily – while still connected to their base office.
- Staff are not limited to working from a specific country – a UK worker could temporarily work from a holiday home in France or Spain, etc.
- Greater use of part-time staff and experts, and individuals (could be self-employed) can be contracted for a specific project on an hourly or daily rate of pay

With greater flexibility and off-site working, it could be difficult to monitor and control staff if they are not all in an office or a central location. There is now a wide variety of online tools and the following types of tools (some platforms could provide some or all of the features)

- **Collaboration tools**

- Allows the sharing of workflows, dashboards and progress updates, virtual to-do lists, progress or time tracking and updates with the team
- May include document upload and storage, and version control
- Examples include Slack, Google Docs, Microsoft SharePoint

- **Communication tools**

- Allows voice, video, instant messaging, email, text, audio and screen sharing
- Work on desktops, laptops, mobile phones and tablets, etc.
- Allows for virtual meetings when the team is more dispersed
- Some businesses are using remote working tools such as Slack as an alternative to traditional email
- Allows the team to propose ideas and solutions to problems and give feedback on the project
- Messages are read when each person gets back to their computer
- It's easy to see when people are online, offline, or busy / in a meeting
- Chat history may be available
- May have file-sharing functionality
- Examples include Slack, Zoom, Skype, Teams, GoToMeeting

**COPYRIGHT
PROTECTED**



- **Scheduling and planning tools**

- Each part of the project can be planned out with time frames and can be updated if progress is slower or faster than expected – can produce Gantt charts
- Tasks can be sent to each member of the team and calendars updated if necessary
- Online calendar functionality to find the best time to schedule meetings
- Staff can add events and tasks to their calendar
- Examples include Outlook and Google calendars, various task management tools

Questions – E1 Online services

1. Give two positive effects of online retail to either customers or retailers.
2. How has online learning transformed education?
3. Give two examples of transactional data.
4. Explain one type of targeted marketing.
5. How do online systems improve teamworking?



INSPECTION COPY

**COPYRIGHT
PROTECTED**



E2 Impact on organisations

As part of the BBC's Computer Literacy Project, a TV series called *Electronic Office* series is well worth a watch <https://archive.org/details/electronic-office> (may also be found at <https://clp.bbcwind.co.uk/27bcf968d0c805c00ee69fbca89931b9>) and gives us a glimpse of the fundamental changes that computers and networks would have on businesses through new ways of working. Bear in mind that the power of computers and the role of networks were unimaginable back in those days!

Use of IT systems in:

Stock control

Knowing the amount and location of stock is one of the most crucial aspects of a business. Businesses need to be able to efficiently locate and manage their products to serve customers in their stores, and be able to price products accordingly. There's no point in keeping vast numbers of items in stock that rarely sell, while frequently running out of the bestselling lines. Many retailers work on a 'just in time' system where new stock is automatically ordered to stores when it is running low. Using a computerised system is much faster than completing a stock check by hand, and allows for a real-time system.

Stock control - Using a computerised system to monitor the amount of goods a company has in storage/warehousing so that more goods can be ordered when they're running out

Visit us IKEA stores

Search by city

Belfast
Hollywood Road
★ In stock

Bristol
Eastgate Road
★ In stock

Cardiff
Ferry Road, Cardiff
★ In stock

The availability of stock is often displayed to customers online so that they know what is available in local stores. Shopworkers also need to know whether a specific item is available when a customer asks for it. Similarly, a library might withdraw books that have been borrowed for years, or move infrequently borrowed items into storage to allow new books to be borrowed.

The stock control system will operate from a large database. Each time an item is added or removed, it can be checked in. This used to be done manually using a handheld barcode scanner, but now as they are scanned all at once, automatically! Each item will have a specific shelf location. Sometimes when you order items online, you'll see the stock location, such as a specific store.

Data logging

Data logging is where data is recorded using a sensor and a data logger, and is either stored locally or transmitted to a server in real time. This can be done without a human being present. The data can be transmitted across the Internet (for example, across the mobile network) or recorded onto a memory card. There have been lots of different data logging devices developed, for example, in the monitoring of volcanic activity or for recording the amount of water in a river. When they are used in real time, they can be used to inform important decisions, and to send warnings or alerts.

Data analysis

Once data has been collected (either manually or automatically), it can be processed and analysed. That can be done manually or automatically; for example, a report or live-dashboard could be updated. The example dashboard below provides real-time information about a company's web servers, which could be a useful tool for the system admins if there are complaints of poor performance, or if there is a higher than expected level of web traffic that could indicate a denial of service attack.

**COPYRIGHT
PROTECTED**





Ask a parent or guardian whether they use loyalty cards for supermarkets or other stores. Do you think the data generated through the schemes is processed?

General office tasks

General office tasks are carried out every day in millions of offices around the world. Basic tasks include using word processors and spreadsheets, emailing clients, and tasks involving web browsers. There are also the back-office uses such as processing invoices and payroll, accounting and all other tasks required to run a business.

General office tasks are carried out every day in millions of offices around the world. Basic tasks include using word processors and spreadsheets, emailing clients, and tasks involving web browsers. There are also the back-office uses such as processing invoices and payroll, accounting and all other tasks required to run a business.

Can you imagine calculating staff payroll for a business with a thousand staff? Or lines in the middle of a page of handwritten text? IT systems, that are networked across a business, mistakes to be quickly corrected, and precise calculations.

Creative tasks

There is a wide range of **creative tasks**, e.g. producing high-quality advertising, video and animation production and CAD (computer-aided design) as well as architectural design and images. All of these benefit from the use of specialist software, templates and downloadable fonts and add-ons. They can make much more elaborate designs in a fraction of the time it would take to do them by hand, and quickly change our minds or create new versions. A good example is the use of 3D printing in prototyping during the design process.

Creative tasks are carried out every day in millions of offices around the world. Basic tasks include using word processors and spreadsheets, emailing clients, and tasks involving web browsers. There are also the back-office uses such as processing invoices and payroll, accounting and all other tasks required to run a business.

Advertising

Brands are using new ways to retain existing customers and find new customers, including innovative augmented reality, QR codes in adverts, and through product placement on TV and by sponsoring YouTube videos.

Advertising is carried out every day in millions of offices around the world. Basic tasks include using word processors and spreadsheets, emailing clients, and tasks involving web browsers. There are also the back-office uses such as processing invoices and payroll, accounting and all other tasks required to run a business.

**COPYRIGHT
PROTECTED**



Manufacturing

Manufacturing now uses a lot of computer-controlled equipment and machinery (numerical control) lathes and other tooling/cutting equipment. These machines work more precisely than by hand, making them a big advantage in the workplace.

Security

Technology allows for security to be increased. There are many different types of physical and logical; for example, biometric and other door control (including key cards, alarms and CCTV. Some of the access can be monitored remotely, and some technology

Impact and implications of IT systems

While many of the impacts and implications of implementing and using an IT system are online systems, the IT system as a whole could be a lot more important, forming the backbone and the platform for the online services.

User experience

Many users are operating the system for many hours each day. A computer system that doesn't work well or breaks frequently, takes a long time to mend. At the end of the day, a computer system is a tool to do a job. You would complain if you saw when building a fence.

- **Ease of use** – is the system easy to use, or are there too many buttons to press something that's non-standard (such as using the shortcut Ctrl + C to close a window)? Is the interface consistent and intuitive? Does it help you keep running if you make a mistake?
- **Performance** – is the system nice and fast (and, therefore, you feel productive) and often freeze or crash? When you're doing technical support and the user is slow, you need to be able to work out whether the actual computer is slow or if it's related to network speed or the response time of online systems.
- **Availability** – is the system available whenever the user needs it? Is part of the system working to a tight deadline and information/services is/are unavailable, they are not available.
- **Accessibility** – the system must be adjustable and accommodating to anyone who uses it. This includes software or settings within the operating system for things such as screen readers and other technology. Hardware could include Braille devices, as well as microphones and speakers for voice control and narration.

Employee and customer needs

Any new system, or change to an existing system, needs to be carefully chosen so that the needs of staff are met (i.e. they can do their jobs as easily as, if not easier than, before), and the standard of customer service is met.

Cost

The cost of implementing a new system could run into thousands or even millions of pounds associated with the purchase and installation of the equipment or software. Other costs associated with training staff and maintaining the system – fixing bugs in the system, troubleshooting issues and replacing failed components.

Implementation

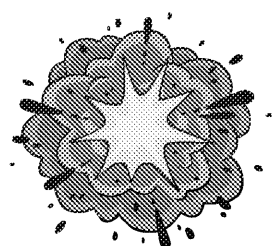
When an organisation chooses a new system (ranging from new software to entire new systems) there are several methods that they could use, depending on the amount of acceptable risk.

The **pilot method** is the slowest and most cautious approach. This is where the new system is tested on a few users; for example, to a single department or subset, or to only one location. This gives the opportunity for issues to be fixed, and the system can be tweaked to optimise it. If pilot testing goes well, then the system can be rolled out to all users with a high level of confidence.

**COPYRIGHT
PROTECTED**



In the **parallel method**, the new system is set up before the old one is taken away. If there are problems with the new system for all or some tasks, the users can switch back to the old system. There are also advantages such as training, which can take place at a slower, more comfortable pace, reducing the staff workload.



With the **big bang method**, the old system is removed and replaced at once; for example, over the weekend, or during a holiday or system shutdown. This can save money but can be the riskiest as there is no ability to quickly fall back on the old system. Staff must learn the new system quickly, which could be a challenge if the new system is very different from the old one.

Whichever method is used, the new system will be tested to ensure that all requirements are met and compatibility is maintained with the existing parts of the system. The timescales set for each part of the implementation – planning, procurement, installation, testing, and training – will vary.

Replacement or implementation with current systems

An IT system is likely to have evolved over many years. Due to the cost and complexity of upgrading or replacing a system, new servers will be purchased when needed, or a new operating system will occur when the older version becomes unsupported or insecure. A company might have outgrown current infrastructure, and a wide-scale change is required.

When adding a new part to the system, it is very important to check that years' worth of data in the new system, or that older software is compatible with new hardware or a new operating system. Physical ports are available or can be adapted to work.

Upgrade work should be planned to avoid busy periods, and might take place during a weekend.

If you're interested in a career in IT, take a look at some of the tools available for system installations; for example, you could check out the Office Deployment Tool, Microsoft Deployment Toolkit, etc.

Productivity

In a well-designed system, the productivity (output for a unit of time) should be high. The system is responsive and the correct software for the job is used, and all necessary tools are available.

Working practices

The system should meet the demands of the business; for example, staff working on different shifts and across different time zones as appropriate.

Staff training needs

Whenever a new system or a new piece of hardware or software is installed, existing staff need to be trained how to use it. This will be the same for anyone who joins the company after the system is installed. This initial training will include how to use the basic functions. Over time, ongoing training will be needed for the additional features of the software. Training could be done in small groups (either on-site or online), or one-to-one (e.g. for more advanced features). Sometimes, representative users might provide some training.

User support

Large companies usually have an in-house technical support department which deals with problems. There is a hierarchical support system with first-line support dealing with the majority of the problems. If they can't deal with the issue by visiting the desk or using remote desktop software or talking the user through a resolution, the issue will be passed to second-line support (and eventually to third-line support).

Users can get help from people who provide services, such as documentation, telephone support, etc.

**COPYRIGHT
PROTECTED**



support, for the most difficult issues to fix). There are fewer people at each level of support. Many people enter IT as first-line support. They use a ticketing system, write notes and see it through to resolution. Fixing is also prioritised – a small issue that affects the workflow of the user is far less urgent than if nobody in a particular office can access a system.

Smaller companies may not have their own internal technical support and will employ a service provider (an external company who looks after the issues). They may have a contract that the issue will be resolved within a fixed time frame, called an SLA – a service level agreement. If the issue is not resolved within the agreed time frame, the service provider could be fined for breach of contract.

Online communities can be used to great effect for user support, with users reporting their issues to support staff or, sometimes, volunteers will respond. The public nature of these communities means frequently asked questions (FAQ) can be answered and made available to all users. Such communities will sprout up spontaneously, as users support each other.

Off-the-shelf, popular software such as Microsoft Office is well furnished with user guides and forums. For example, if a user needs to use a more advanced part of the software, the available resources will be extensive. If the software is bespoke (i.e. has been custom written for the organisation), documentation and procedures will have been created.

Security

Whenever a new system is implemented, or equipment is added on, there will always be a security risk. We've already covered the basics of security. Staff will need to follow any accepted security policies. If necessary, follow any procedures to ensure that security is maintained.

Questions – E2 Impact on organisations

1. How can electronic systems improve the efficiency of stock control?
2. Suggest two possible systems where data could be transmitted and logged. Come up with two of your own suggestions.
3. What is the role of testing when a new IT system is being implemented?
4. Explain why staff need both initial training and ongoing training.
5. An employee has a problem with their machine. How could they ensure the problem is resolved?

**COPYRIGHT
PROTECTED**



E3 Using and manipulating data

Having quality information is important to stakeholders – that's anyone who has an interest in a business, and includes staff, customers and **shareholders**. Some of the people may have invested their own money into the business, if they have purchased shares. They needed quality information before they bought those shares to assess whether those shares were worth buying, and need continued information such as company reports and finance information, otherwise they might sell those shares.

Those managing and making important decisions at the top of the businesses need to have large amounts of up-to-date and accurate information at their fingertips. They need to know that the business is profitable, that targets are being met, which lines are selling well, and those which are not. They need to know the state of the market, which trends are taking off, and which are declining. There's no point in paying for information if nobody is buying, while a competitor launches a brand-new product and storms the market.

Knowing this information allows the business to stay profitable, explore new sales and new growth strategies. If their business is less profitable, they need the information to identify a problem and quickly solve it.

Sources of data

Primary data and secondary data

In your Geography class, you might have stood outside a shopping centre to ask shoppers where they travelled from, or sat at the side of a road counting cars. This is **primary** data because YOU collected it, for a specific purpose. Primary data can come from surveys and questionnaires, focus groups, interviews and from a census.

Primary data
organised by
a supervisor
and collected

In the same way, a business can collect primary data. This data might be captured as it is generated, through an online survey sent out to customers, or information produced by the business. The business knows exactly how that data was collected, understands the strengths and weaknesses of the collection, and can ask very specific questions (or run specific queries from a database) that perfectly fits with their task.

Secondary data, however, is data that has been produced by someone else for a different purpose. For example, a company might purchase secondary data to complement its own data – to see whether their findings match other people's data or conclusions, or to provide another data set to compare to, perhaps for a similar product or field.

Secondary data
bought or
does not

Secondary data can be much cheaper to obtain, since it is collated by specialists or organisations – it is cheaper to buy a copy of a report than to spend hours or days collecting data. Secondary data can be more readily available than primary data; however, as there is less certainty over its reliability, and they might find it irrelevant or misleading.

Here are some common secondary sources:

- **Books** – a wide range of published material including data tables, analysis, etc. Sometimes you might use the other person's conclusions to compare with your own, or to spend more time doing some original research (time-consuming) – for example, to study climate change and read the diary of a scientist written 200 years ago.
- **Government reports and statistics** – a wide range of statistics are available from government websites, trusted. You can usually download spreadsheets or CSV files containing raw data, and charts are also included. Websites usually have a search function so that you can easily find what you need.

**COPYRIGHT
PROTECTED**



- **Magazines and journals** – including periodicals and scientific literature. The literature review to see the research that's already been done (no point duplicating what students spend a whole year doing this! The articles also tell you about other people's findings and results. Appendices may publish summaries of the data that was collected.
- **Websites** – beware of the age, bias and validity of the data. Anyone can create a website, probably safer getting data from a site such as a university or a government.

Judging and ensuring the reliability of data

Take a simple quiz question such as 'What is the most common pub name in the UK?' That seems like a very easy fact to check – just find every pub on a map, and tally them up in a spreadsheet (until you realise just how many there are!). If you search the Internet, the common response is that it's 'The Red Lion', but one site says that there are 47 pubs called 'The Red Lion', another 543 (close!), but one says 584 (nowhere near!). Some sites tell you that 'The Red Lion' is the second most popular name, while others say it's the most common.

So why is there so much variation even for such a simple question?

Accuracy – we don't know who compiled the data behind those statistics. It could have been an official body, such as a government official keeping track of landlords' licences, or it could have been anyone on the Internet who accidentally forgot to include a few here and there.

Always be wary of where information came from; for example, an online encyclopaedia that anyone can modify, it could be a personal opinion presented as fact, or someone misunderstanding or misremembering something that they had read elsewhere. If you look at online technical support pages, you'll see all sorts of 'fixes' that won't work, are bad advice, or are just what someone didn't understand the topic enough and wrote what they thought was right, or who used a certain word in the wrong context.

Bias – maybe the person didn't like a particular town or city and chose to exclude it, or increased the number of the name they liked – a bit extreme, but you get the idea.

Bias is where you project your views or preferences into your writing. Perhaps you like one political party over another. You might write only positive things about the party, ignore its failings, or maybe you don't write anything positive at all about the parties you don't like. Writing a product or film review and don't mention the negatives. Biased writing is everywhere.

A manufacturer won't tell you about the bad things about their product because they don't want to hear about those parts on the review sites.

Information can become **out of date** if the circumstances around the data have changed. For example, information about those pubs was compiled 10 years ago. During that time, pubs have changed, new owners might change the name of the premises. (Of course, just because information is old doesn't mean it's not useful. Old data can be vital. For instance, if you want to predict the weather for the winter months because you'd want to see how well ice cream sales are doing.)

When we use online sources of data, we should always check that it's likely to be up to date, or we can't rely on it to make informed decisions.

**COPYRIGHT
PROTECTED**



Methods of data collection

The fundamental to information management is **collecting** information. This can be done in a number of ways:

- an online questionnaire, survey or sign-up form – this information can be recorded automatically
- a paper-based questionnaire, or notes from discussion, interviews of focus group – the notes can be entered into a **database** system later
- information downloaded from the Internet
- printed material, including books, reports, letters, etc.
- ideas and understanding provided by the staff within a business

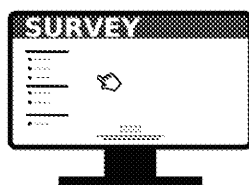
Data
data

Survey

Surveys are often used to gauge an opinion. A survey is usually a short set of questions.

Survey
main
ques
follow

Customers or anyone who is signed up to mailing lists are sent links to online surveys. Up on platforms such as SurveyMonkey for minimal cost. Sometimes there might be a chance to be entered into a prize draw as compensation for your time. You may be asked to complete a customer satisfaction survey when you dine out or go shopping – details are often used so the business uses your feedback to improve its service.



Surveys might be shorter and less detailed than questionnaires. They often use closed numerical, binary or limited-choice questions. Open questions, such as an optional box asking for any other comments, are also included. Questions include ranges (e.g. on a scale of 1–5, 1 being very unsatisfied, 5 being very satisfied). Writing questions without bias can be tricky, so it's important to be an expert and test your questions on a few people before using them to check that they understand the questions.

Questionnaire

A **questionnaire** is a set of questions that are given to customers or a small sample of the public – similar to a survey, but often they're longer and more likely to be given in person or over the phone. For example, a developer might send a questionnaire to residents in the streets surrounding the proposed new building, or university students might be asked to complete a questionnaire to select a sample of residents (e.g. every other house in a street) for a coursework project.

Questionnaire
a respo
quali
online

Interviews may have more open questions to allow for more open discussion. The rapport with the questioner which could lead to better participation (but could also lead to bias in what the interviewer wants to hear). The questioner can also judge misunderstanding, confusion, and can rephrase or adjust the questions if necessary.

Focus groups

You may have seen a focus group on the TV series *The Apprentice* when the candidates were given a notoriously bad product to a group of people, and a lot of (some deserved) negative feedback ensues – maybe we're mainly shown the bad bits for the purposes of the show. If you don't watch that show, a focus group is where a group of around 10 people are invited to meet at a specified location to test and discuss the advantages and disadvantages of a product under the supervision of a moderator. The people chosen for the focus group should be familiar with the product they are testing/discussing – there's no point selecting someone for a taste test of an item if they don't eat, or asking someone who doesn't cycle to test a new cycle helmet, etc. There may be a mix of people, and they might be previous customers or express an interest in being part of the study.

Focus group
to disc
e.g. w
suita

**COPYRIGHT
PROTECTED**



Interview

An **interview** is a formal discussion between the *interviewer*, who asks open questions and makes notes on answers, and the *interviewee*, who responds to the questions. Most of this data is *qualitative*, i.e. words rather than numbers (*quantitative*). This means that it is harder and more time-consuming to transcribe or input, but the level of detail and depth is much better. Interviews can be conducted in person, via webcams, or just over people because of the high costs and long process. Here are two examples of why

- Undertaking *detailed research* to gain better depth. Interviews are useful before a form or survey, allowing further questions and details to be provided. The interviewer with the interviewee allowing for openness, and is able to gauge whether the questions, rephrasing questions if necessary and changing later questions.
- A *job interview* – while paper forms, CVs and cover letters are great for whittling down candidates to the few most promising ones, interviews are nearly always necessary. Sometimes there is a telephone or virtual interview first, followed by a face-to-face interview. A business will spend a lot of money hiring you to do the job, so they want to be sure that you are reliable, honest and trustworthy (and will hopefully stay with them for a few years). Interviews allow the candidate to elaborate on what they've said on their CV and impress the hiring manager. But job interviews work both ways – the candidate gets to ask questions too, finding out exactly what the job involves and to get a feel for the company and its culture.



Inter
betw
asks
Frequ
purpo

Reasons for ensuring data accuracy

In order to make the correct decisions based on information, the information must be accurate and unbiased – we must have a full, overall picture. It's difficult to satisfy all of our needs in limited amounts of time checking things, but we should do the best we can. Remember, 'garbage in, garbage out'. If you put incorrect, out-of-date or incomplete information into a system, the resulting sales forecast isn't worth the paper that it's printed on.

Methods of ensuring data accuracy

Verification and validation

Data **validation** is a way of making sure that the data that is inputted makes sense and is correct if it appears to be valid and in an expected format or tolerance. If we are entering data into a system, the system might check that they all start with 07. If we're typing in dates of birth in the format 01/01/2000, there shouldn't be any letters.

Data **verification** is slightly different. It is a check that the data is correct and can take place when the data is initially entered (e.g. if you need to change a password you'll need to type it in twice to check it matches both times) or a further check later on (for example, to make sure that customer contact details on file remain up to date). Sometimes we verify that data remains intact when we copy it by comparing the copy to the original.

Validat
correct
checks
contain

Verific
inputte
type in
might ne

Data verification

Here are two methods for checking that the data inputted is correct.

Double entry – simply typing in the same data twice and checking that both inputs match. It involves two people to type in the same data independently and checking for a match. If the data doesn't match, it will need to be entered a third time. But as this takes at least double the time, so it's not always the best for business. This reduces possible errors such as typos or human error.

Here are some examples:

- When you change your password you'll need to type in the new one twice to make sure you didn't make a mistake – this saves you needing to reset it again.
- When typing in handwritten data sets – to make sure there are no typos or errors.

COPYRIGHT
PROTECTED



Manual checking is a laborious and time-consuming task. Another person checks

- This resource will have been proofread by an expert in the English language – grammatical errors – the stuff that spellcheck misses, and to ensure that the Simple errors are corrected automatically, but if there's anything that is unclear will go back to me, the author, to correct.
- An expert in the field will also be asked to read this work to check for mistakes and recommendations. In the academic world, this is called *peer review*. Before they are given to several experts to pick up errors and holes in arguments or journals are accurate and can be relied upon to be as correct as possible.
- In business and government – documents, forms and IDs are checked by someone out to the customer. If you get a prescription from your doctor, the box from the dispenser, and one from another pharmacist that they all match what the doctor prescribed. An error could prove fatal.
- Sometimes businesses will contact customers using alternative details on the records are up to date. This may be done when letters are returned to the sender. For example, a business staff might phone up the customer, or use a second email address.

Data validation tools

A **data type check** checks whether the data entered is in the correct type, e.g. text box, only numbers are entered into numerical fields, etc. This would indicate the wrong fields in a database, for example. Checks could take place as the data is run on a database to flag any instances.

Format checks and input masks check whether the data entered is in the correct combination of letters or numbers. This is achieved with the input mask – using a pattern to determine the correct format and number of characters entered.

A **length check** checks either that the exact number of expected numbers has been inputted, or that the number of characters within a specific range has been inputted.

For example, if you were measuring something where the answer is always three digits, the check would be for anything other than three digits. But for something like a postcode, where you could have either 5 or 7 characters, that range should be allowed. In reality you might want to use 5–8 characters for the check as people often leave the middle of each postcode – some won't, so the minimum still needs to be 5.

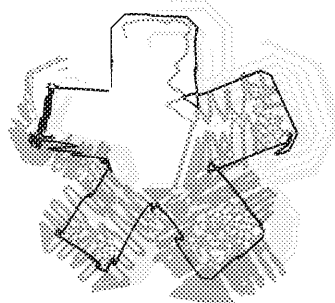
Limited choice – when there are only a few (most important) options that can be allowed for quicker input, and standardise the answers for someone looking at the data. For example, online surveys, questionnaires, forms and when making purchases online; for example, expiry dates and checking the box to say that you have read the terms and conditions.

Here are three types:

- **Drop-down lists** – for example, when entering dates you will have numbers for month, day and several years as drop-down. Addresses might have a list of countries or counties.
- **Radio buttons** – only one of several options can be selected. If you try to select a second option, the first is deselected (think of an old radio or TV with physical buttons – if you change the channel, then the previously selected button pops back up).
- **Tick list** – when you need to select two or more options. The first two options remain selected, unlike radio buttons.

**COPYRIGHT
PROTECTED**





A **presence check** simply checks that something has been entered in a field (but the presence check itself doesn't check the value). When you use online forms, you will often see an asterisk (*) to indicate that some input must be entered. If you miss this, the page won't let you continue when you click submit. It will inform you which field you need to complete in order to proceed.

A **range check** is a check to remove data that might be outside of an expected range. Maybe you made a typo. For example, if I entered my age into a form as 150 years old, that would be outside the expected range and therefore, rejected.

Sometimes you may just be given a warning when entering data so that you can correct it. Let's say that you are entering your family name into software and the software expects it to take place between the years 1800-2000, but you have a great aunt who married into a family that was accepted before this is outside the expected range in case you miss it. Being 150 years old isn't!

Methods of extracting and sorting data

Spreadsheets and databases are often used to extract and sort data.

Retrieving the information can be as easy as opening up a spreadsheet or document and navigating to the correct tab or section of the document. In a database, the information can be selected using a **query**. This will output all of the data that matches certain criteria; for example, the email address of each customer who has signed up for a service in the past month so they can be sent a newsletter, or a list of customers who have not paid their bills on time.

Of course, most businesses still collect and store information on paper. This method is very inefficient – paper is bulky and must be located and retrieved manually. Instead of someone quickly opening a file while sitting at their desk, they must walk to the filing room and sift through folders, files and pages to retrieve the information.

A lookup is a function in spreadsheets which is formula-based. It can be used to retrieve data from a cell from somewhere else in the spreadsheet. This saves a lot of time and reduces the risk of copying data, and means that the value only needs to be updated once if a mistake is made.

Specialist software can also be used, that can also produce reports.

Sorting the data arranges the data in a particular order; for example, you could sort values from largest to smallest, or categorise the data. You have probably used this in Excel many times before.

Numerical and data manipulation

Once the data has been retrieved, it must be processed. This is a way of making the information easier to understand or read. For example, the information could be sorted or moved around – **manipulated**. The information could also be **processed** – for example, displaying the information in a chart.

Modelling is using that sales data to generate new information. For example, previous data could be used to project the number of future sales, or to change different variables to see what happens – what-if analysis. While useful, these models might not be accurate, and they cannot forecast major events such as recessions and global pandemics. Of course, during a global pandemic, complex

**COPYRIGHT
PROTECTED**



models are used to forecast the number of cases given different scenarios. These models advise the government on the effect of different policies such as the timing and level of models can be assessed by comparing the output to real data. For example, if you could ask it to forecast data in the twentieth century, which we have a good data set for.

Analysing information

Analysing information is about working out what it means; for example, using the patterns – is there a 'correlation' or relationship between two variables? A supermarket might notice that much extra ice cream people buy depending on the temperature outside – it uses this past sales information to quickly increase the amount of ice cream in its stores in a sunny weekend.

Presenting data and results

There are lots of ways that we can present the data. We often incorporate the data into projects and reports.

Presenting data in tables and spreadsheets

Tables are rows and columns of printed or displayed, tabulated data. They are used to present a large amount of information, but they can be difficult to interpret.

They are used in company balance sheets, reports and accounting records, and in scientific experiments, and included in journals and other scientific and technical websites. They display numbers, but many tables also display text.

Tables can also be displayed in a **spreadsheet**. Spreadsheets can be large stores of data in rows (across) and columns (down), while each data point is called a 'cell'. Spreadsheets are software (e.g. Excel, or Pages on the Mac) which are used to store and display data (including mathematical formulae) and are used to make calculations and analyse the data.

Spreadsheets are used by businesses to perform thousands of different functions.

The first ever spreadsheet software was called Visicalc (visible calculator) and was developed on the computer, the Apple II, in 1979. It was so popular for generating sales projections that many businesses purchased that computer just to use the spreadsheet! What-if analysis was possible in seconds, rather than hours of manual calculations. Some of those first projections were inaccurate, based on the data that was fed into those early spreadsheets!

Charts and graphs

We have all produced and seen charts and graphs, which are visual representations of data. You've probably drawn them out on a sheet of graph paper, or used a spreadsheet to show the results of a science experiment, or from fieldwork data.

We use the terms 'graph' and 'chart' to mean the same thing – but there's a slight difference. A **graph** is technically the output of mathematical modelling, while a **chart** is just a way of displaying data.

There are lots of different types of chart, such as bar, pie and scatter – different types of chart will be appropriate for the type or format of data that we want to display.

Charts can be used to show trends in data that would be difficult to spot in a table, or show two charts side by side to compare them.



**COPYRIGHT
PROTECTED**



For example, we could use:

- pie charts to show percentages or proportions
- bar charts to show and compare different categories
- histograms (like a bar chart but each bar touches the next) to show change over time
- scatterplots to compare two variables
- line charts to show a trend between two variables

Finally, to present a summary of data, e.g. for a presentation or for a general audience on your organisation's social media, an infographic could be produced: a visual summary of key data.



User interfaces used in data collection and processing systems

When collecting data, it is important that the interface is well designed, or errors occur. For example, if members of the public enter data online, staff enter data into a system over the phone, or waiter entering customer orders for the kitchen, or just

Ease of use

The forms for data entry should be clearly and consistently labelled, using appropriate text and clearly designed buttons and drop-down menus. Remember that if someone is filling in a form, they want to do so as quickly as possible or they might get frustrated and give up. The form might have a 'next' or 'submit' button, but with the ability to go back if they have changed their mind.

If a customer services representative is typing in order details while a customer is waiting, the interface should be quick and easy – they don't want to keep the customer waiting, or make any mistakes while they are speaking to them about something else.

Here are a couple of examples:

The passport application uses a very simple layout – radio buttons, a continue button. There's also an important information box, written in very clear English.

The Aldi survey gives a series of boxes that correspond to blocks of numbers printed on a receipt. There's a 'Next' button. To make it easy to find the number on a long receipt, a marked example is provided.

Accessibility

The layout and text should be legible to people with disabilities. The large print version of the passport application are good examples. There's also good contrast and no colour

COPYRIGHT
PROTECTED



Error reduction

Errors are reduced by using radio buttons, drop-down menus, calendars and other types of typing in the material (you could make a typo or type something unexpected). Verification checks that we've already discussed could be used.

Intuitiveness

Some interfaces are so easy to use that the user requires very little or no training. For example, it's very obvious that you need to click either 'Yes' or 'No', and then confirm that so intuitive, especially if they are unfamiliar with using a computer or the type of interface.

Functionality

The interface must include all of the features that are necessary or required by the user, related to the underlying technologies used to create the site or the skill of the user.

Performance

The online survey must be able to input data, and having a fast, reliable web server to load instantly, with no errors or timeouts, or the user will get frustrated and abandon the survey.

Compatibility

The software or web page should work on a wide range of devices. A lot of older users are still reliant on Internet Explorer (IE). Once Microsoft stops supporting IE, those users need to be migrated to newer browsers. Some functions don't work as well in different browsers, so developers must ensure that all of the users can complete the survey in their browser. It should be used by the public.

Questions – E3 Using and manipulating data

1. Give one source of primary data and one source of secondary data that you have used in part of your studies (any subject).
2. A company is testing a new product with the public. What type of data collection is most effective, and why?
3. How can we ensure that data is inputted correctly?
4. Explain one use of data modelling.
5. An employee needs to produce a report and visually represent how sales change over time. How could they do that? Give an example.

**COPYRIGHT
PROTECTED**



⑥ F: Issues

In this chapter you will learn:

- ① The moral and ethical factors in the use of information technology, and professional codes of conduct
- ① The legislation that affects computer systems
- ① That professional guidelines exist

F1 Moral and ethical issues

Moral and ethical factors of the use of information technology

The terms **ethics** and **morals** are often used interchangeably. It is helpful to differentiate between good behaviour (morals) and an ethical code which is often based on moral principles. So a business will:

1. Adhere to the law
2. Follow a code of ethics if it exists for their industry
3. Be affected by the morals of the leadership of the businesses

Ethics – principles

Morals – and unacceptable

One difficulty is that often the law hasn't caught up with technological changes, and laws are not developed enough to have a universally agreed code of ethics, yet technology has a great deal of power and influence.

Everyone's morals are slightly different (unique to each person); for example, what is acceptable between what is and isn't acceptable. Therefore, someone may not believe that they will still follow the ethical code.

Privacy

Throughout the world, people are becoming increasingly concerned over companies and governments watching their online footprint – the web pages they view, the messages they send, and who they send them to. This is the reason why people use VPNs to hide their Web surfing, and encrypted messaging services such as WhatsApp. However, governments and law enforcement are becoming increasingly concerned because encryption also helps fuel criminal activity. Encryption isn't a bad thing – it's essential for safe online shopping and banking – it's just that if two criminals are conspiring to commit a crime, the police can't foil it as easily.

In isolation, a single piece of information isn't too much of a concern. However, it is when it is used to build up a detailed profile of a person. Your computer data may be collected and stored (often in the small print that you often agree to without reading). They may track your movements, devices. For example, shopping patterns, location, cookies, and identifiable information. They may work out where someone lives, their age, their sex and gender identity, any health issues, if in debt, their hobbies and interests and whether they are married, etc.

In general, governments have sweeping powers to monitor citizens, reducing individual **privacy**. For example, number plate recognition cameras are installed along motorways, and installed in police cars. In the future, real-time facial recognition software could track individuals in public areas and when they visit certain shops and locations, or even commit minor offences.

Privacy – the right to be left alone; the right to be free from intrusion into one's private life; the right to control one's own information.

Facial recognition software could also be used to identify race, and be used to control access to certain areas. It explains: <https://www.cnet.com/news/in-china-facial-recognition-public-shaming/>

INSPECTION COPY

COPYRIGHT
PROTECTED



Environmental

As our population grows, and countries develop, the impact that we have on the environment increases. We are consuming more resources and energy than ever before, meaning that we are causing significant and perhaps irrecoverable damage to Earth's life support systems and our climate.

IT includes all of the computers and devices in the homes and offices all over the world – but there is also hidden uses of energy – all of the cloud servers, the Internet and communications networks that operate 24/7/365, and the transport used by the communications companies.

About half of the CO₂ generated by IT is generated by the equipment in our homes and offices. The other half is used by the data centres and the distribution network.

But we must also consider other environmental factors across the entire **product life cycle** – including:

- the metals and rare earths mined – water pollution and habitat destruction – remember that IT electronics use rare materials from all over the world
- the plastic required and their disposal
- water used in the manufacturing process
- transport of materials, product and waste products
- the paper and ink, and other consumables used by the equipment
- disposal of the products, including recycling

The carbon footprint is the amount of the gas carbon dioxide (CO₂) that a person produces. The problem with CO₂ is that it's a greenhouse gas. The more we add to severe the level of climate change (global warming) will be.

We generate CO₂ when we burn fossil fuels such as coal, gas and oil. Many countries generate electricity from coal and gas – and all IT equipment requires electricity. Even in the worst polluter, coal, but gas is still our largest source of electricity.

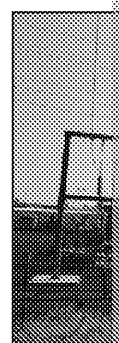
IT produces around 1.4 % of the global CO₂ emissions. The company Ericsson published a report that looked at the carbon footprint of IT equipment between 2010 and 2015. Despite a 50% increase in transmission over that period, they concluded that very little extra CO₂ was generated.

We can reduce the carbon footprints by ensuring that new equipment is energy-efficient (powerful (processing) but use less energy than before – computers run a lot cooler) and we have seen major shifts in the IT industry towards lower-powered devices:

- Switch away from high-power consumption desktops to laptops
- Switch from CRT monitors to LCD displays – the LCDs were initially using fluorescent bulbs so still got fairly hot, but now they use very cool and efficient LED backlighting
- Switch towards tablets and smartphones
- Improved energy efficiency and software control
- Increased virtualisation and online applications – processing power is server based, and thin-client computers can be used

However, in the last few years we have seen an even greater growth in the use of cloud services, online applications and use of streaming TV services – so we are in danger of offsetting those positives on the consumer equipment side.

You may have heard that Facebook opened a data centre in Luleå, in northern Sweden. Microsoft experimented with a small underwater data centre capsule – putting a data centre in the ocean makes a lot of sense because data centres need a lot of air conditioning to keep cool.



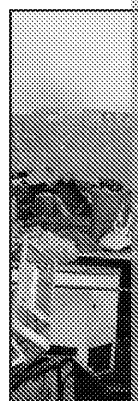
Data centre

**COPYRIGHT
PROTECTED**



The underlying principle of sustainability is meeting the needs of the present without affecting the ability of future generations. We can translate this into IT through:

- ✓ Reducing the amount of materials required to make new products – some of the metals used to make smartphones are only mined in a few specific locations and the resources are finite.
- ✓ Ensuring that products can be repaired and upgraded, rather than needing to replace all of the equipment – again, reducing the amount of resources used.
- ✓ Ensuring that hardware remains supported for many years, and that new software updates are released – to stop a fast upgrade cycle (built-in obsolescence).
- ✓ Ensuring that products are energy-efficient to reduce the impact on climate.
- ✓ Promoting donation of working and usable IT equipment to charities for redistribution.
- ✓ Using less paper and ink (through enabling double-sided (duplex) printing) and less ink/toner on the paper (and using recycled paper).
- ✓ To ensure that the products are easily recyclable – reducing the space taken.
- ✓ Recycling products efficiently in the USA and Europe, rather than sending them to China where disposal can harm the environment and people's health – burning electronic waste, or dumping in landfill.



'Recycling' in Ghana. The image shows the hazardous waste disposal of electronic equipment.

There are many benefits to green IT, which include:

- ✓ Cheaper to run – lower energy costs
- ✓ Cheaper to recycle
- ✓ Ability to work from home – less time spent commuting
- ✓ Enhanced brand image and reputation – most companies have a sustainability policy and they show off their green credentials and environmental management systems.
- ✓ Stakeholders and customers expect it – this is called a 'triple bottom line' of business – go green or lose sales! Greenpeace used to rank the major electronics companies on how green they were.

Unequal access to information technology

The key barrier to communications is the digital divide – between those who have access to technology and those who don't. Those who don't are cut off from the many benefits and conveniences, such as online shopping and access to services. Barriers could include:

- Age – some of our elderly population don't know how to use modern technology, and will perhaps never learn to.
- Wealth – some people just can't afford the cost of devices and ongoing fees for mobile phone contracts.
- Location – some countries still have fairly undeveloped communications networks.

**COPYRIGHT
PROTECTED**



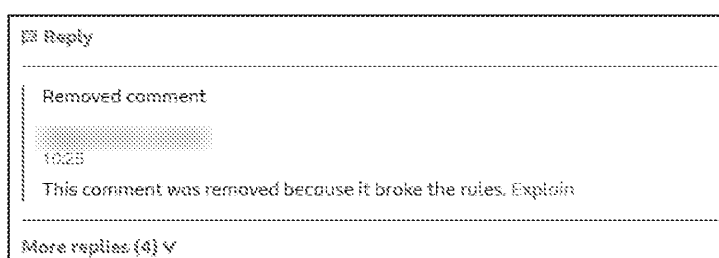
Online behaviour and netiquette

The way that we behave online can affect others. For example, the posts that we make or share on social media and instant messaging, forums and chat rooms, voice chat when gaming online, and email. We are a lot more anonymous online, which means that we are more likely to be offensive than in person, and we often share deep or personal things more easily than in person.

Most of the time, if we cause someone else to be offended, it's not deliberate. The way or what we said has a different meaning in other cultures. However, some people go through cyberbullying, trolling (deliberately causing conflict), flaming (insults and abuse) or flaming (insults and abuse) (creating a fake persona to target a specific person, e.g. to gain personal information). Some people share fake news, either without realising it or deliberately.

Most of us are sensible online and follow a set of rules for being polite – called **netiquette** (net etiquette). The rules are pretty sensible – essentially say generally positive things, without using swear words, and if you wouldn't say something to someone's face, don't write it online. Don't send people spam, breach copyright or hijack a conversation and take it off topic.

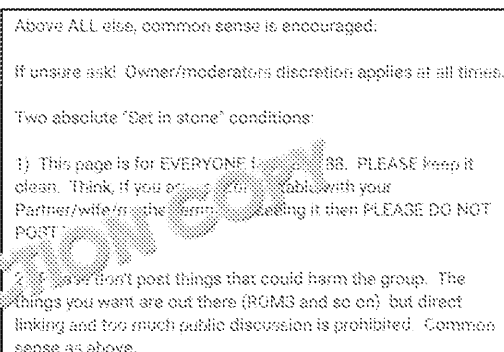
Some online communities, including YouTube comments, use moderators (either people or bots) to check that people follow the rules – if someone writes lines of profanity, the



Here's an example of a comment that was removed because of poor netiquette.

And of course, public groups will have a set of ground rules about what is and isn't allowed. In public Facebook groups, take a look at the rules.

Here's an example of a computer group on Facebook's rules:



Here we can clearly see that the owners of the group are looking for good netiquette and no flaming. The group is also shielding itself from legal issues if people posted direct links to copyrighted material from people with lower moral standards. ROMS were old games or code. Some argue that by sharing them, they are not causing any harm or loss of income to the original creators as they made them many years ago as the material is no longer for sale. That's perhaps a valid argument, but it's also protected by copyright, which you'll read about later.

But they are also advocating freedom of speech – by allowing members to check if their posts are not sure whether something they want to post complies with the group's rules.

**COPYRIGHT
PROTECTED**



Globalisation

Globalisation of technology has brought with it crime that uses the technology – often from different countries and in a way that makes it very difficult to trace. Criminals also use encryption technology to communicate with each other so the police are unable to tap their phones. New laws are being created in many countries to counteract this but many also impinge on people's freedoms – which creates an ethical dilemma for the lawmakers.

There are a number of areas which have ethical trade-offs including:

- Airport full-body scanners – do you want security or privacy?
- GPS technologies – during the coronavirus lockdown, apps were developed to show close proximity to a person who has coronavirus and notify us accordingly – are tracking our movements.
- Technology in warfare – we have reports of American drones killing terrorists in strikes in which some innocent civilians are killed – is this justified?

Some of the challenges of globalisation are being faced by countries working together. Countries are working globalisation by asking other countries to sign up to multilateral agreements. One is the payment of taxes from large multinational companies; another is the fact of having the same access to services.

Businesses are taking advantage of globalisation in the way they have restructured. It's a bit of a joke in Geography that globalisation could be represented by a picture of a Big Mac in China – and there's some truth in this. Large multinational companies can access information around the world at any time of day or night, and expand across new markets. Jobs can be transferred to other countries where wages are cheaper. For example, call centres based in the UK were transferred to countries such as India and the Philippines.

As a result of the global access to information, traditional cultures are changing. Have you watched videos online made by people in other countries? Or watched a Hollywood movie on social media and tried to recreate it? Or chatted online to a friend or family member in another country? It could be argued that we're all becoming more similar – more homogenised – as we adopt other cultures and adopting them into our lives. It's very interesting that regional differences are now much less pronounced than only a few decades ago – TV and the Internet have suddenly see things that would once have taken months or years to spread across the world.

Freedom of speech and censorship

Freedom of speech means that a person or group of people should be able to say whatever they like (providing that it's legal, i.e. not hate crime or racist) without any censorship or fear of persecution. This is a human right under the freedom of expression under the Universal Declaration of Human Rights.

Censorship is where something is blocked from view or suppressed – this could mean blocking a specific website across a whole country, bleeping out swear words during a live online chat, or redacting text by drawing thick black lines through it. Not all censorship is bad though; it's good to block things that are illegal, such as instructions for how to make a bomb, or text that could lead to self-harm or suicide.

Freedom of speech means that a person or group of people should be able to say whatever they like (providing that it's legal, i.e. not hate crime or racist) without any censorship or fear of persecution. This is a human right under the freedom of expression under the Universal Declaration of Human Rights.

Censorship is where something is blocked from view or suppressed – this could mean blocking a specific website across a whole country, bleeping out swear words during a live online chat, or redacting text by drawing thick black lines through it. Not all censorship is bad though; it's good to block things that are illegal, such as instructions for how to make a bomb, or text that could lead to self-harm or suicide.

**COPYRIGHT
PROTECTED**



The Web was designed to be open, but countries around the world are restricting specific sites, and censoring some online conversations. This is a divisive topic.

Here is a map showing how open the Internet was by country in 2020–2021.

Global internet freedom rankings according to government control and censorship*



It is interesting to see such a map, but it's strange how data is missing for so many countries, most Western media access is blocked. In North Korea, very few people have Internet and all use is closely monitored. In China, social media comes in the form of WeChat, a messaging service which lacks strong encryption and can allow authorities to read messages to get around censorship; for example, by blocking VPNs. Some countries also block other messaging services such as WhatsApp over fears that the platform could be used to spread political movements.

It is worth noting that some governments have a variety of laws over allowing citizens to use the Internet. Some countries have laws that allow terrorists and criminals to communicate in secret, and that service providers have to remove harmful content. In 2016, Apple fought the FBI over the refusal to provide an iPhone that was part of a criminal investigation:

<https://www.bbc.co.uk/news/world-us-canada-35692931>

Because of this, some companies go as far as only providing users with very secure communication (called end-to-end encryption), where the keys are stored on the user's device only and cannot be forced by authorities to hand over the communications or encryption keys. They also have access to the keys.

INSPECTION COPY

COPYRIGHT
PROTECTED



To counter this, seven governments signed an open letter in 2020 which you can read at <https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and> governments agree that secure encryption is important for the running of society – online banking – they say *'Particular implementations of encryption technology, however, pose risks to public safety, including to highly vulnerable members of our societies like sexually exploited individuals. We address our serious concerns where encryption is applied in a way that wholly precludes*

However, note the use of the word 'urge' – this letter is not forcing companies to use encryption in the use of services such as WhatsApp. It will be very interesting to see what happens in the next few years.

Acceptable use

An **acceptable use policy** (AUP) sets out what people may and may not use a network, i.e. which uses are acceptable. They mostly focus on what you can't do, so as long as you're legal, doesn't harm others and isn't specifically mentioned, it's probably OK.

AUPs protect the network from attack, abuse, illegal activity and legal liability, and you must use it. You will normally accept the agreement by clicking a box to accept (e.g. signing up to a service) or you may be asked to manually or electronically sign an agreement (e.g. on your first day at work). Somebody else such as your line manager will also countersign.

You may agree to be bound by acceptable use policies in lots of different scenarios:

- using your school, college, or university network
- using a computer system at work
- using a public Wi-Fi connection in a café or holiday home, or on the bus or train
- purchasing a subscription for a home broadband connection
- signing up to a social media site
- downloading apps
- accessing or signing up to general websites, including forums

Each AUP varies depending on the specific scenario. Some common don'ts in an AUP are:

- No downloading or uploading of illegal material (e.g. indecent images of children or material) or copyright infringing content
- No hacking or malware distribution
- No activity that degrades the network performance for others (e.g. 24/7 file sharing)
- No spamming or sending unsolicited email (especially if you've been asked not to)
- No online bullying, defamatory or racist messages
- Don't let someone else log in to the system or your account, log in as someone else
- No copying the content of the website

There are different sections within the AUP. For example, the sections cover:

- **Scope** – what the policy applies to, e.g. staff and students at the college
- **Assets** – what the policy covers, including files and information
- **Acceptable** – anything that is allowed (if specified) or anything that users are allowed to do
- **Unacceptable** – anything that is not allowed
- **Monitoring** – how compliance is monitored, e.g. logs, web filtering, tracking
- **Sanctions** – the processes to investigate and the potential penalties for breaches
- **Agreement** – how you will accept the policy – tick box, (electronic) signature

**COPYRIGHT
PROTECTED**



Purpose and role of codes of professional bodies

When organisations develop digital systems, there may be industry guidelines they should follow. The NHS Digital has a framework that sets out core standards on technology and data by which all systems in the NHS must abide, which will also affect private companies creating software to be used in the NHS.

On the other hand, social media companies do not have a framework, and there have been several initiatives that have not gone far enough to keep users safe, that the UK government introduced a new framework in March 2022 as the Online Safety Bill.

Impact of codes of practice on individuals and organisations

Ethical decisions need to be considered at an early stage by the top decision-makers in the company where it affects the cost and the design of a product. In the same way that a company building houses should have ethical consideration for people who lose their homes, companies running chemical factories should have ethical considerations for disposal of chemical waste in a safe way, so companies building digital systems have consideration of their users' health and safety.

Social media platforms building digital tools for easy communication should consider the potential for communication for paedophiles who prey on children, and for trolls who send many people for no good reason, and there have been cases of Internet users encouraging others to commit suicide. Companies building encryption tools may have those tools used for illegal purposes.

Questions – F1 Moral and ethical issues

1. Give one example of a moral issue and one example of an ethical issue.
2. Why are some people concerned about privacy?
3. What are the environmental issues associated with cloud storage?
4. Give one example of good netiquette and one example of bad netiquette.
5. Suggest two threats to a free Internet.

**COPYRIGHT
PROTECTED**



F2 Legal issues

All information holders (including businesses) must comply with the laws, and speed of change. Companies who are abroad must also be aware of the laws in the countries they operate in. As companies become more global, they will face greater challenges as they move across borders.

The fines for businesses who do not comply with the laws can be very severe. For GDPR is €20 million or 4 % of annual global turnover – whichever is the higher. A list of fines given out by the ICO here: <https://ico.org.uk/action-weve-taken/enforcement>

Current legislation (with amendments)

If you read books about IT from perhaps 40 years ago, they would say that your computer was a handful of computer systems. That's probably true, but today – and now those computers are connected to the Internet, potentially allowing hackers access to that data. The more places your data is stored, the greater the chance of a breach.

Your personal information is valuable because it can be sold on the dark web to cybercriminals for identity theft and other fraud. Identity theft is particularly problematic because criminals can open accounts and loans in your name and it can be very difficult and time-consuming to convince them you didn't set up the account. At best, you could receive more scam calls, junk mail, and credit card statements.

Computer misuse and Police and justice

Computer Misuse Act 1990

In the very early days of computing, there were no laws against hacking, meaning that it was difficult to prosecute hackers using the existing laws – sentences were typically light, if charges were possible. However, the law has since caught up with hackers and criminals.

The first laws were introduced in 1990 in England and Wales with the Computer Misuse Act 1990, with separate provisions in Scotland. This law made three things illegal, punishable through fines and prison time:

1. Unauthorised access into a computer system
2. Unauthorised access into a computer system with the intention to commit further offences
3. Unauthorised modification of files

Since 1990, the offences have changed slightly and the penalties have become more severe. The Digital Economy Act 2010 has been introduced – now up to 10 years in prison and larger fines. These changes were made in the **Act 2006** and the **Serious Crime Act 2015**.

Under these amended acts, the following are now criminal offences:

1. Unauthorised access into a computer system (finding weaknesses into the computer system)
2. Unauthorised impairment of a computer system (including modifying or deleting data, or causing a system to crash)
3. Making, supplying or obtaining materials to use in acts of computer misuse (including hacking tools and malware)

Fighting cybercrime is difficult – many crimes committed go unpunished because the perpetrators are not located in the UK, so prosecutors need to partner with authorities in other countries.



**COPYRIGHT
PROTECTED**



Copyright, designs and patents

Copyright law protects works from being copied, published or performed by others. Copyright includes books and printed publications, music, film and television, and other artistic works. All material is automatically covered, and generally cannot be copied until 70 years after the author's death (although there are limitations and different time periods, and it is slightly different for material created for or by a business).

If you find out that somebody else has reproduced your work, such as copied paragraphs of text from your book into theirs, you can sue for breach of copyright.

If a company wishes to publish an extract of copyrighted material, they generally need to ask permission from the owner – the 'rights holder'. The owner might give permission, or ask for a fee. Sometimes a small amount of the work can be published under the protection of 'fair dealing' or 'fair use', but this can only be used for criticism or review. For example, you could display a short TV clip and discuss weaknesses. You could also use an extract in a review – but that's as far as it goes. Some people either by revoking their copyright claims and releasing the material into the 'public domain' or through the Creative Commons or a similar scheme.

For education and private study, you can usually photocopy 5 % of a book, for example.

Similarly, if you uploaded photos and video to social media, you would be pretty much adding it to their profile or website. You must be very careful what you post online, as printed material, websites and posts are usually under copyright. For example, you could add a link to your profile, rather than taking a screenshot and re-uploading it to your own. The copyright logo – © – as many people and businesses will add it to the corner of a photo.

It's also worth taking a look at the terms of use of the social media accounts that you probably skipped through and said that you read...). For example, Facebook tells you the rules for your photos (<https://www.facebook.com/terms.php>). Remember that anything you post on your friends' newsfeeds, so be careful what you post.



Go to [zzed.uk/11526](https://www.zzed.uk/11526)

Copyright regulations (computer programs)

Computer programs (and online content) are covered under the Copyright (Computer Programs) Regulations 1992 (from 1st January 1993). This law stopped you from distributing or selling copies of software on a network. But you were allowed to make a single copy of the software. Back in the 1980s, software was often purchased on floppy disks. Because the disks were fairly fragile, the first thing you would do was to copy the disk – it was expected that the copy was your daily working copy. If the original was damaged or corrupted, you would create a new copy of the original.

Display screen equipment health and safety

Many workers look at a display screen for the majority of their working day. Display screen equipment includes desktop computers and laptops, but nowadays also tablets and mobile devices. Employers must ensure that staff are kept as safe as possible while in the workplace.

- General health and safety falls under the Health and Safety at Work Act 1974.
- Working with IT equipment is covered under the Health and Safety (Display Screen Equipment) Regulations 1992, which remains largely unchanged.

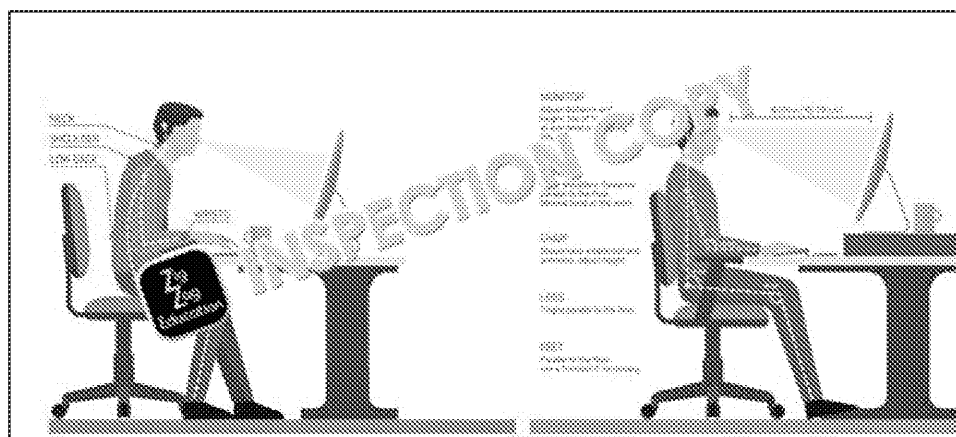
Under the display screen equipment regulations:

- Workstation assessments – employers must check that the workstation is correct when the employee starts the job, changes desks or a change is made to the workstation, and regularly.
- Employers must allow staff to take regular breaks from the screen, which could be as simple as making phone calls and attending meetings. There's no specific guidance, but a common rule is five minutes every hour.

**COPYRIGHT
PROTECTED**



- Employers must pay for eyesight testing if staff request it (either by arranging by reimbursing staff). The employer must also pay for glasses, but only if the staff are using the screen.
- Employers must provide training on things such as good posture, adjusting chairs, taking breaks and reporting issues. Remember that many offices now use adjustable desks, so staff can choose whether to sit or stand at different times of the day.
- Staff temporarily working from home – while a full workstation assessment is not possible, check that staff have a good workspace. If they work from home permanently, a full assessment is required.



Data protection legislation

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

Because of the danger of hacking, and the importance of keeping personal data secure, we have legislation in place to help protect it – for example, the Data Protection Act 2018 and General Data Protection Regulation. These regulations protect how data can be collected, stored, used and protected.

The new legislation was stricter than the old, and gave citizens greater rights on data held on them, consenting to the use of their data, and having their data removed. When the new legislation came into force in 2018, everyone received emails from dozens of companies they had signed up to over the past decade or more, asking for permission to retain the data. Many of these emails had pre-ticked boxes to sign up to receive marketing emails, for example.

The penalties for non-compliance and for failure to protect data (e.g. breaches) have been set the bar high – the maximum offence was the larger of either €20 million or 4% of annual turnover. In the UK, the euro price was converted to £17.5 million, and fines are handed out by the Information Commissioner's Office.

Below are the general principles of the Data Protection Act 2018 / GDPR (which replaced the Data Protection Act 1998). The UK was still in the EU when the GDPR came into force, so it became law in the UK.

Lawful processing

The person in overall charge of the data and sets how it is processed is the data controller. The employees who use the data on a day-to-day basis are the data processors. They must ensure that the data is used (processed) only as instructed by the data controller. The controller must ensure that the processing has a 'legitimate interest' to the business, and that the person who the data is about (the data subject) has given consent for their data to be used.

Data protection
methods
being
– by
by

**COPYRIGHT
PROTECTED**



Collection for a specific purpose

The data collected must only be used for the purpose that it was collected for – no chooses to collect data, it must decide what data to collect, and why that data is ne use that data for a different purpose, it may need to ask for consent again.

Only necessary collection

The minimum amount of data should be collected – only what is absolutely need relevant for the study. If you are a volunteer taste testing a new bar of chocolate, company would need to know your mother's maiden name or your National Insur legitimately want to know your age and your gender because that information w for marketing if a bar of chocolate was particularly well-received by a certain dem

Accuracy

The real world is complicated and changing frequently. For example, we move hou (and may change surnames), have children, etc. The data might be accurate (corr collected, but after a few months, or years, it might be inaccurate.

This could lead to inaccurate, misleading or incorrect decisions to be made based legislation, businesses should be very clear on where the data was collected from make checks on the accuracy if necessary. If the data is discovered to be incorrect corrected (or deleted) as soon as possible.

Only kept as long as necessary

In most business settings, except for archiving and statistical analysis, it is unlike keep your personal data indefinitely. If you've bought something online, keeping your last purchase probably isn't necessary. In that case, the company should ann its data is still relevant, and delete or anonymise anything that's no longer neces have a standard data retention policy, informing the data subject how long their

Data subject rights

Remember that the data subject is the person whom the data is about. The data rights to (be):

- Informed – about how and why their data is being collected, the privacy and
- Access – anyone can request to see a copy of the data that is held about the a month of the request. (Note that this is different from a Freedom of Inform for information from a public organisation, such as a local council.)
- Rectified – any incorrect data to be corrected, and any incomplete data com
- Erasure – in some cases, you may request that a company deletes certain da the data is inaccurate, used only for marketing, is being used for a different
- Restrict processing – stop the data being used for some purposes (a substit
- Portability – take a copy of your data to another service (previously discusse
- Object – stop the data being processed in certain circumstances, e.g. market
- Automated decision-making/profiling – e.g. important decisions made by personal circumstances, in account. The data subject may be able to ask a made made to be overturned.

Protected

All of the personal data must be adequately protected from hackers, data breach the business must have sufficient equipment (e.g. firewalls), antivirus software, e in place to prevent breaches and ensure that the data is safe. After the data and necessary, the data must be destroyed, e.g. by shredding paper and tapes, magne

Companies risk large fines if their systems are breached or if their protection me ICO of the breach within 72 hours of discovery, as previously mentioned.

**COPYRIGHT
PROTECTED**



Not transferred to countries with less protection

Not all countries have the strict protection laws afforded by the Data Protection Act. Flows of data are essential to our modern lives.

This is why when you try to access some websites – for example, where the site is blocked in your country – they are blocked from access. Companies that operate across the world might have data in different countries and not transfer that data to others. In 2020, a judge in Ireland (where Facebook has its European centre) ordered Facebook to stop transferring any data about EU citizens to the U.S.

While companies may reach agreements that any data transferred will be treated with the same protection as U.S. Privacy Shield is no longer valid at the time of writing, meaning that this is not the case. Data transferred to the U.S. is not protected. Does this mean that using Google Analytics, for example, is not a good idea?

Consumer rights legislation

The Consumer Rights Act 2015 gives you extra protection against poor-quality goods and services. If there's a problem, you can get a full refund for purchases made less than 30 days after purchase. If the problem is more serious, for 1–6 months, and after six months, the same applies, but you can get a repair or replacement rather than a refund. This 30-day refund doesn't apply to downloads, though.

The three requirements for the product are:

- Fit for purpose – capable of doing the job it was sold to do
- As described – meets the description or model number
- Satisfactory quality – in working, undamaged condition when sold (although this is judged based on price and expected lifespan of the device)

Current accessibility legislation (with amendments)**Disability and equality legislation****Equality Act (EQA) 2010**

This act aimed to stop discrimination, victimisation and harassment, and to bring together different anti-discrimination laws. The act means that you as an employee or an individual in public life should not be treated differently against for things such as your age, your gender, your sexual orientation, etc. This includes direct discrimination – how you are treated – and indirect discrimination, e.g. a policy that applies to everyone but disadvantages a particular group. For example, when you apply for a job, an employer can't reject you because of your skin or your sexual orientation, whether you have a disability but are perfectly capable of doing the job, or whether you are likely to need maternity leave in the next few years. Failure to comply with the act can lead to court proceedings and fines if found guilty.

This means that the use of technology should not discriminate, nor should anyone using technology for any of these.

One simple example is that websites should be readable by screen readers so that people who are visually impaired are not discriminated against.

In 2006, the United Nations Convention on the Rights of Persons with Disabilities was adopted. It states that, instead, the focus should be on everybody else – 'subjects', who just happen to live with disabilities. Everyone should have equal rights with non-disabled people, as they should be given the same access to information in order to make decisions. It is also argued that access to the Internet, is a human right.

British Standards Institution (BSI) codes of practice

The British Standards Institution was set up in London over 120 years ago. The group sets standards for products which mean that products made by different companies all adhere to the same standards. This means they are interchangeable, and all have the same safety standards.

**COPYRIGHT
PROTECTED**



You have probably seen the BSI logo many times without realising it; for example, metal covers in the street and many electrical cables use the famous 'Kitemark' – a triangle with a 'B' on top and an 'S' in the middle. (When I was growing up, I thought that this logo represented electricity itself, based on the S, which I saw as the sine wave, used to represent alternating current!)

The BSI covers many different industries. Along with the general management of customer service and environmental standards, within IT we're probably most interested in:

- Biometrics (implementing biometric systems)
- Data protection (personal information management systems)
- Electrical and electronic (quality in consumer electricals)
- ICT and telecoms (managing networks and improving customer service within)
- Information management (safe and secure information use)
- Internet of things (currently in development – take a look when you read the

You can see the full list and take a look at each standard here:

<https://www.bsigroup.com/en-GB/industries-and-sectors/>



Open Accessibility Framework (OAF)

OAF guidelines provide a series of 'steps' to ensure that any computing platform these are set out for developers to allow the software to be accessible to people platform. The steps for the developers include:

- A definition of accessibility, and how this translates to each platform.
- Providing stock elements of the user interface (how users will interact with)
- Providing tools to create the application.
- Providing support for the development platform.
- Providing the actual application software that is accessible.
- Providing various assistive technologies that work with the app (such as magnifying screen allowed, and allowing alternative input methods).

Web Content Accessibility Guidelines (WCAG) and World Wide Web Consortium (W3C)

The World Wide Web Consortium (W3C) was set up by the creator of the Web, Sir Tim Berners-Lee, in 1994, just three years after the Web's development. It sets out the standards that should ideally be used with the Web, such as encouraging each organisation to implement the same version of the language used. If there were major differences between each version, the Web would look different.

Part of the W3C is the Web Accessibility Initiative (WAI) which publishes the Web Content Accessibility Guidelines (WCAG). There have been several versions of the guidelines since 1999, and by 2008 it may be the standard. Compliance isn't always enforced, but the European Union has a public body that tests websites and apps conform to the standards.

There are many different ways suggested to make the content available to people with limited sight (appropriate colours and text narration), deafness (subtitles and transcripts), limited hearing (alternatives to voice input) and limited movement (input and navigation without a mouse).

The principles of WCAG 2 are:

- Perceivable (alt text and alternative formats, alternatives for time-based media, and easy separation between the background and foreground).
- Operable (use keyboard-only navigation, provide time to read content, avoid seizures, and allow navigable, searchable content).
- Understandable (all text should be understandable, websites should operate without user mistakes / allow for easy correction).
- Robust (compatible with assistive technologies).

You can use checking tools from W3C to check the compliance and accessibility of a website – it could be a web page you've created – and copy the HTML content of a 'source' or similar) then paste it here: <https://validator.w3.org> (or <https://jigsaw.w3.org>).



Question 2 Legal Issues

1. Give two examples of crimes under the Computer Misuse Act 1990, with permission.
2. If you wish to reprint material that someone else has created, why do you need permission from the rights holder?
3. How does the Data Protection Act affect you personally?
4. How does the Equality Act protect against discrimination?
5. Why are standards such as WCAG needed?



INSPECTION COPY

**COPYRIGHT
PROTECTED**



Answers

Learning Aim ①

Section A1

1. Multifunction devices have more than one use. A laptop has many different applications to web browsing, gaming and other entertainment, such as watching videos.
(2 marks)
2. Allow any suitable example, and any use, e.g. games console for playing games or streaming platforms.
(2 marks)
3. A smartphone is connected to the Internet, which can provide real-time updates on accidents and roadworks – not always possible with a stand-alone satnav.
(2 marks)
4. Any two examples such as online retail and click and collect (customer side), inventory control and automated ordering systems, or creating a large database.
(2 marks)
5. e.g. a server (could specify a type, e.g. domain controller), which is not part of local or Microsoft accounts are typically used. Allow other specific hardware such as scanners and label or receipt printers that are typically only used in commerce.
(2 marks)

Section A2

1. Any suitable suggestion such as a touchscreen which is used to control the system's visual output.
(2 marks)
2. Automatic data processing saves a lot of time over manually inputting data; there are fewer errors and corrections are likely.
(2 marks)
3. Any two examples, e.g. screen reader, OCR (optical character recognition) device.
(2 marks)
4. Any two backup media such as tape or hard drive because of the low price and the media is cheap, the amounts of data that now need backing up mean that optical media is not suitable.
(2 marks)
5. Any two benefits that allow the replacement of magnetic media applications (e.g. floppy disk), low energy consumption, very fast access times (e.g. SSD).
(2 marks)

Section A3

1. The original types would really be a graphical user interface running on a computer. CLIs are not suitable for most tasks in the modern world because most modern applications are graphical. Real-time and single-user single task are used only in specialist applications, not every desk within an office, for example. Multi-user could work; for example, many desktops on a single server.
(2 marks)
2. The operating system is crucial in interfacing between the hardware and software written for specific operating systems. The OS also provides many valuable tasks and network connections, which are used by the applications.
(2 marks)

INSPECTION COPY

COPYRIGHT
PROTECTED



3. Utility software perform small background functions and tools that are used or software are used for the main tasks of the computer, and are used directly by processor used to produce this resource.
(2 marks)
4. Open-source software can be used in a wide range of commercial applications modified to suit the exact requirements of the user.
(2 marks)
5. JPEG because it produces small files due to the lossy compression / photos are text to use lossy compression.
(2 marks)

Section A4

1. An autonomous robot uses sensors to have an awareness of its surrounding or decisions. Any suitable example, such as a device used to pick online orders in industrial applications.
(2 marks)
2. The car would need to make life-or-death decisions, potentially choosing whether pedestrians, or decisions that could lead to serious injuries.
(2 marks)
3. Business – e.g. training staff to operate machinery or systems. Entertainment
(2 marks)
4. Driverless cars need to be taught what every potential object that they encounter learning, the control software must learn to recognise different objects.
(2 marks)
5. Lack of standards, lots of sensors, e.g. microphones and cameras, outdated software personal settings.
(2 marks)

Section A5

1. Any two advantages, e.g. increased efficiency, easy to correct mistakes, central communications, and data synchronisation.
(2 marks)
2. Any two disadvantages, e.g. single points of failure such as a failed switch or a power cut to the whole office, RSI and potential eyesight deterioration, and maintenance costs, and security concerns / data breaches etc.
(2 marks)
3. Implications of the system on the user, such as how easy the system is to use and accessibility.
(2 marks)
4. It is unlikely that the whole system will be replaced at once – the new part needs to be able to import all of the existing data.
(Or, that the new system must be able to import all of the existing data.)
(2 marks)
5. Any two explained aspects such as a time frame for implementation, testing of which staff are migrated to the new system.
(2 marks)

**COPYRIGHT
PROTECTED**



Learning Aim ②

Section B1

1. Wireless is more flexible (devices anywhere without wires), but the performance could drop.
(2 marks)
2. Satellite because it is available anywhere where there is an unobstructed view, use cable are unavailable / too remote for a reliable mobile signal.
(2 marks)
3. Core network infrastructure, external and internal because of the extremely high demand where there is a lot of electromagnetic interference.
(2 marks)
4. The router provides the interface between the external public Internet, and access on the network to a specific IP address.
(2 marks)
5. Allow a discussion on bandwidth of the incoming supply, speed symmetry, and latency.
(2 marks)

Section B2

1. Any two ways that PANs and LANs vary, e.g. size (PANs much smaller), the type of equipment and fixed equipment more likely on a LAN / portable devices and peripherals, protocols (Bluetooth on a PAN, Wi-Fi and Ethernet on a LAN).
(2 marks)
2. Linking together resources shared in a head office with the branch offices; connecting from a central location.
(2 marks)
3. Remote working, such as connecting back to the office, and increasing security of connection, such as in a café.
(2 marks)
4. Any suitable arguments over cost, e.g. the type of external connection, or when internally link switches together.
(2 marks)
5. Any two suggestions, e.g. resort to paper, without files and information, many things are back online.
(2 marks)

Section B3

1. A protocol specifies the rules for transmission, such as information about the sender and receiver.
(2 marks)
2. POP (allow POP3) and IMAP. Do not accept SMTP as the email is sent TO the server.
(2 marks)
3. Any two examples of VoIP, e.g. a video call with friends and family, or a voice over IP phone, or out to customers.
(2 marks)
4. Must use the HTTPS protocol, which encrypts the network traffic.
(2 marks)

INSPECTION COPY

COPYRIGHT
PROTECTED



Learning Aim ③

Section C1

1. Any two: no large upfront costs, scalable (increase and decrease as required), (electricity, maintenance) as all managed by the hosting company.
(2 marks)
2. Accessible anywhere so can be accessed off-site or in branch offices, allowing on location. Also allow discussion based on groups of people working collaborate tools.
(2 marks)
3. Mobile devices could easily get lost, so storing photos to the cloud allows them to be lost. Also allow discussion that in business, items such as email, contacts and documents are backed up. Using the cloud is automatic and much easier than having to connect to a server.
(2 marks)
4. A VPN (Virtual Private Network) is an encrypted network tunnel that allows you to connect to a remote device (locally), whereas a remote desktop allows control and use of a remote computer installed on the remote device.
(2 marks)
5. Cloud server because mobile devices could be lost / cloud servers have very high security.
(2 marks)

Section C2

1. Any two possible reasons, with a wide scope, e.g. relating to giving too much scope for bullying and cyberstalking, etc., or answers relating to social media taking up too much time.
(2 marks)
2. Very short and may need to span several messages; therefore, could be misunderstood. Message in such a short time, limited educational value.
(2 marks)
3. Any two differences, e.g. chat rooms operate in real time and are private, whereas social media are often public.
(2 marks)
4. Any two reasons about how social media could damage a company's reputation: negative complaints left by disgruntled customers, accounts could be hijacked by hackers.
(2 marks)
5. Any two reasons, e.g. paid for by advertising, cost is giving over personal data for services, users would switch to a rival platform.
(2 marks)

INSPECTION COPY

**COPYRIGHT
PROTECTED**



Learning Aim ④

Section D1

1. Two reasons, e.g. self-replication and stand-alone program for worms, where they are attached to other files.
(2 marks)
2. The hacker is not trying to cause deliberate damage or steal personal data / is just warn the owner about (moral), but the activity breaches the Computer Misuse Act. He asked permission to test the system (illegal).
(2 marks)
3. The damage was not deliberate or malicious; hacker's error / accidentally pressed a key.
(2 marks)
4. Any two problems, e.g. time and difficulty involved in resolving the issue, cost of the system.
(2 marks)
5. Any two consequences, e.g. loss of reputation and potentially customers, fines, loss of lost advantage.
(2 marks)

Section D2

1. Some information (such as payroll and accounts) is confidential and should not be shared. Or, commercially sensitive data should be seen only by the fewest people possible. Or, deliberate leaks.
(2 marks)
2. Disaster recovery policies ensure that the data can be restored if there has been a disaster. If a building has been destroyed. Restoring data from a backup is essential in this situation.
(2 marks)
3. Tokens could include a USB dongle or key generator, or a mobile device to receive a code for authentication process. These are not available to a hacker, so most logins that require a token will fail.
(2marks)
4. Hard firewalls will be used at the gateway to reject unsolicited data packets and soft firewalls help prevent the spread of malware from an infected machine within a network.
(2 marks)
5. Asymmetric encryption is more secure / much harder to crack because of the use of two different keys.
(2 marks)

INSPECTION COPY

COPYRIGHT
PROTECTED



Learning Aim ⑤

Section E1

1. Customers – ease of use / convenience / 24/7 shopping. Retailers – cheaper reselection of customers.
(2 marks)
2. Any two examples of online education, e.g. VLEs, online examinations, MOOCs.
(2 marks)
3. Any two examples, e.g. generated at the till – prices, payment type, loyalty card transactions, as well as back office and service desk applications.
(2 marks)
4. e.g. email marketing to a mailing list of existing customers, or customers who targeted social media advertising. Alternatively, the company will target specific demographics.
(2 marks)
5. Allow any suitable or explained example of online systems and modern teamwork collaboration tools, shared online documents that allow multiple authors, Voice over IP, instant messaging, etc.
(2 marks)

Section E2

1. Continuously up-to-date log of all stock and its location, combines sales data and can be automatic.
(2 marks)
2. Any two plausible suggestions from the learner, e.g. anything with an online data source generated by a solar PV panel, or the data generated by a weather station.
(2 marks)
3. To ensure that the system meets all of the needs and compatibility before installing the system slowly to provide feedback from the staff, as well as testing post-installation that the system works as designed and success criteria have been met.
(2 marks)
4. Initial training – how to use basic features so that staff can do their core roles and then in how to use the more advanced features.
(2 marks)
5. Log the issue with the service desk at the company using the reporting process. The service desk will then take ownership of the issue and escalate it if it cannot be resolved through the service desk.
(2 marks)

Section E3

1. Any suitable example based on the learner – now in a list have been collected and obtained from an online source.
(2 marks)
2. Focus group because all people involved have an interest in the product / device and can discuss it in detail.
(2 marks)
3. Any suitable form, such as double-entry, manual checking, but also allow error checking, e.g. range/format/length checks.
(2 marks)
4. Any suitable use, e.g. to predict the change of something over time, such as climate change.
(2 marks)
5. Use a chart, e.g. a line graph or a series of bars.
(2 marks)

INSPECTION COPY

**COPYRIGHT
PROTECTED**



Learning Aim ⑥

Section F1

1. Moral issue – something that is personal, such as deciding behaviour; ethical standards and practices. Any suitable examples of each, following those two points.
(2 marks)
2. Any two, e.g. combining data, identity theft, keeping private things private.
(2 marks)
3. Electricity generation required to keep the servers running 24/7 – which, if generated, increases climate change.
(2 marks)
4. Any one example of good netiquette, e.g. being polite and helpful, and any one example of bad netiquette, e.g. flaming, causing distress, bad language.
(2 marks)
5. Any two issues such as full government censorship / control of the Internet, specific websites / intercept messages, etc.
(2 marks)

Section F2

1. Any two clauses under the Computer Misuse Act, and amendments such as unauthorised impairment, spreading malware, etc.
(2 marks)
2. The work is covered by copyright – it would be illegal to simply republish some of it without their permission / paying royalties (unless the use falls under fair usage or fair dealing).
(2 marks)
3. Any two suggestions based on the control of personal data, such as being able to opt out of mailing lists, or knowing that data will be sufficiently protected if it is stored.
(2 marks)
4. The Equality Act ensures that people are not discriminated against (action that applies to the workplace and to public places).
(2 marks)
5. To provide a framework for developers to make high-quality, accessible products (based on standards from the learner).
(2 marks)

INSPECTION COPY

COPYRIGHT
PROTECTED

