- A digital device is a piece of physical equipment that uses digital data.
- Personal computers are general purposes computing devices like desktops and laptops. They're relatively small and inexpensive and are commonly used in the workplace for tasks like word processing, desktop publishing, etc. They're used at home for the web, email and gaming.
- Servers are used to manage access to web pages, email, files & printers. They're similar to personal computers but usually contain more storage, faster processing, greater memory & an active network connection.
- Mobile devices are digital devices that are designed to be portable by being compact, light-weight and running on battery power. They're most commonly used for internet access.
- Entertainment systems are devices that are used purely for the purpose of entertainment, such as watching tv, listening to music & playing games. They usually have good storage & internet connectivity as well as a number of features specific to each device.
- Navigation systems are devices that use GPS to locate you on a map and plan routes to a chosen destination. It is commonly used as an in-car satnav to plan your route while driving.

Digital Devices 1

Digital Devices 2

- Multifunctional devices are capable of more than one function, such as input and output. They're used for many different reasons, such as touch screens that allow you to input data without a separate keyboard, and force feedback game controllers that let you control the game while receiving vibration as output.
- Digital cameras are used to take photo and video and store it as digital data. This can then be used to share the photos and videos online or to edit them using photo or video editing software.
- Data capture and collection systems input and store data through methods other than direct data entry. They're commonly used in shops at the EPOS till, such as barcode scanners for inputting products.
- Communication devices and systems move data between two other devices, such as two computers. We use them for networking, including to send and receive data over the internet.

- Output devices are used to send data from a digital device to a user or another device.
- Monitor – A device that outputs a visual display of the user interface of any software that is currently being used on the computer.
- Projector – This projects a visual display of the user interface onto a wall or screen.
- Printer – A device that is used to produce physical copies of the documents & images produced using a computer system.
- Plotter – A type of printer that is designed to print out vector graphic images. It typically prints to a very high quality on very large paper.
- Speakers – A device that is designed to produce audio output by converting the digital audio signal from a computer into an analogue signal.
- Actuator – An output device that produces motion. We use it to control or move things.

creative tasks.

- Creative Task uses of digital devices include 3d graphics, photo/video editing & graphic design. This has made it much quicker and easier to perform common reducing staffing numbers and travel requirements.
- Organisational uses of digital devices include administration, video conferencing & design and manufacturing. This has helped save businesses money by both businesses and customers.
- Retail uses of digital devices include EPOS, stock management & online retail websites. This has made buying and selling products much more efficient for

Uses of Digital Devices 2

4 of 43

Uses of Digital Devices 1

3 of 43

- Education & Training uses of digital devices include interactive whiteboards, virtual learning environments & online learning websites. This has made education more easily accessible, even from home.
- Personal uses of digital devices include entertainment, online shopping and banking & home appliances. This has helped save us lots of time in our personal lives by automating tasks and saving us from having to travel as much.
- Social uses of digital devices include social networking sites, instant messaging & VoIP. This has made it much cheaper and easier to keep in touch with our friends and family.

Input & Output Devices

Input devices are used to allow us to enter information into a computer system. For example:

- Keyboard – Made up of a panel of keys, this device is used to input alphanumeric characters, symbols and simple commands into a computer.
- Mouse – A pointing device that allows a user to control a cursor on the screen in order to select objects that are displayed.
- Microphone – An audio input device that allows a user to enter sounds into the computer system.
- Webcam – A device used to input digital video or still pictures into a computer system.
- Game Controller – Used to control video games, this can come in a gamepad form or in the form of a joystick.
- Sensor – An input device that takes readings from the environment such as temperate or light.
- Scanner – A device that converts documents into digital data so that they can be viewed and edited on a computer system.
- Graphics Tablet – A flat board and a pointing device, known as a stylus, that allows a user to enter data much like they're using a pen & paper.

Storage Devices

Hard disk drives are a form of magnetic storage commonly used as the primary storage devices in a computer system.They have a large storage capacity and are reliable as they have a long lifespan.

However their read/write time is slow compared to SSD, can be easily damaged by knocks and are not particularly portable when compared to alternatives.

Solid state drives are a form of flash storage often used as a portable storage device with a large capacity. They're also used commonly as primary storage in mobile devices, laptops & recently desktops.They have fast/read-write speeds compared to HDDs, consume less power than HDDs and are not easily damaged by knocks.

However, they are comparatively expensive compared to HDDs and as such generally have a lower storage capacity. They also have a limited number of writes.

USB flash drives are a form of flash storage commonly used for transferring data between different computers, as well as to back up our files.They are very portable, are durable to knocks and are very compatible with devices.

However, they are easily lost, have a limited number of writes, and have a comparatively low storage capacity.

SD cards are a form of flash storage commonly used in digital cameras, as well as in mobile devices like smartphones.They are very small and portable and are also reliable as they aren't easily damaged by knocks.

However, they have a relatively small capacity and there can be some issues with comp

Optical disks, like CDs, DVDs & Blu-Ray, are a form of optical storage commonly used fo

tv & software, for distribution by suppliers.

th most personal computers and are highly portable.
However, their storage capacity is relatively small and they can be easily damaged.

Data Processing & Accessibility Devices

7 of 43

Manual data processing involves an individual entering data into the computer themselves.
For example, this could be a hotel entering customer booking details or a teacher marking examination papers or coursework.
Automatic data processing is where the role of data entry is taken away from individual users.
For example, this could be OMR used for lottery tickets or smart readers in homes to monitor energy use.
Manual data entry is good at handling complex data and requires less training. However automatic data entry is more accurate, quicker and cheaper.
Accessibility devices are used to aid people with disabilities in accessing the information on computer systems.
Examples include trackballs, braille keyboards, large key keyboards, touchscreens, braille embossers, screen magnifiers and eye typers.

Types & Role of Operating Systems

8 of 43

- There are four main types of operating system. Real-time, single-user single-task, single-user multi-tasking and multi-user operating systems.
- Real-time operating systems process data as soon as it enters the computer system allowing it to respond immediately to input. We see it used in traffic lights, manufacturing robots & air traffic control systems.
- Single-user, single-task operating systems can only be used by one person at a time, using a single application. They were used in old mobile phones and PDA devices.
- Single-user, multi-tasking operating systems are designed for only a single user at a time, however, it can run multiple applications simultaneously. This is commonly used in general purpose computing devices like smartphones, tablets and PCs.
- Multi-user operating systems allow many different users to make use of a computer system and its resources at the same time. This is commonly seen used in powerful servers, supercomputers and mainframes.
- The role of the operating system includes networking (TCP/IP, Network Utilities), security (anti-virus, firewalls, user authentication), memory management (assigning memory to different applications), multi-tasking (allowing multiple applications to run at once) & device drivers (software programs that allow peripherals to communicate with a computer).

- It fits the needs of users very effectively but it can be time-consuming to adapt the interface to individuals.

- An adapted interface is one that will alter its presentation, layout & even options in order to better support the user or the technology it is running on. This is often used to adapt a GUI to suit the needs of those with disabilities.
- This is very easy to use and easily adapted to different users. However, it can be frustrating to complete tasks if there are many levels of submenus.
- A menu driven interface presents the user with a menu with a list of options. This is used in self-service kiosks such as ATMs.
- It is quicker to complete many tasks for experienced users that know the commands and requires very little processing power, memory and storage. However, it is very difficult to use for beginners.
- A command line interface involves a plain background with a simple text prompt that would allow you to enter in commands to perform actions. It was commonly used in older systems where processing power and memory was limited. It is still sometimes used by experienced users, especially for networking tasks.
- It is easy to use and is easy to move data between applications, however, it uses a lot of processing power, memory & storage. It can also be slow to complete tasks for experienced users.
- A graphical user interface is designed around graphical icons and images. It is commonly used on personal computers & smartphones.
- The user interface is the way in which users interact with a computer system.

Choice & Use of User Interfaces

Performance of Operating Systems

- Some of the factors affecting operating system performance include the hardware available, malware & virtual memory.
- Hardware is an issue where you don't have enough memory for the operating system & applications running.
- Malware, such as viruses, will corrupt data and take over O/S functions to hinder performance.
- Virtual memory being used excessively can lead to thrashing. You also might not have a large enough pagefile.
- Utility software are small programs designed to help manage and maintain your computer system.
- Disk Defragmenter, backup, disk cleaner, registry cleaner, software update, anti-virus & firewalls are all utility software we use to keep our system running effectively.
- The utility software performance can be negatively affected by things like a large or fragmented hard disk, applications running in the background, slow network connections and malware.

- Application software is what allows the end use of an IT system to perform tasks.
- Productivity software is used to allow users to perform their work-based tasks more efficiently. Examples include word processing, spreadsheet, database & presentation software.
- Graphics/multimedia software is used to produce graphics and multimedia products on your computer system. Examples include CAD, graphics editing, desktop publishing & video editing software.
- Personal software is used in the home to help in our general lives. Examples include home finance, educational & entertainment software.
- Communication software is used to allow users to share information by passing it from one device to another. Examples include email, web browsing, VoIP & instant messaging software.
- Choosing application software usually comes down to compatibility, use & user experience.
- Compatibility is whether it works with your current hardware & software, use is whether it has the required functionality & user experience is whether the users are able to use the software comfortably.

Application Software

Image & Video File Types

- File types define the kind of data that is being stored in a file.
- File types can greatly affect the compatibility, file size & quality of videos and images.
- Image file types and their uses include:
  - BMP is used for high-quality images, like photos.
  - JPG is used for high-quality images, like photos, that are to be shared over the internet.
  - GIF is used for simple images on the web, like logos.
  - PNG is used for high-quality images that require transparency.
  - SVG is used for vector graphics and can be displayed on a web page.
- Video file types and their uses include:
  - AVI is used for high-quality video, often during production.
  - MP4 is used for playing videos on mobile devices and for internet streaming.
  - MOV is used for internet streaming.
  - MKV is used for HD video, commonly downloaded over the internet.

viruses.

Implications of Emerging Technologies

- Emerging technologies are technologies that are just starting to make an impact in the wider world.
- IT systems often require much more powerful capabilities to handle emerging technologies. E.g. Tesla self-driving car computers are 40 times more powerful than previously used.
- Examples of emerging technologies in our personal lives, or soon coming, include smartwatches, smart speakers and self-driving cars.
- The advantages include the convenience and accessibility, the disadvantages include the cost and over-reliance on them.
- Examples of emerging technologies in business, or soon coming, include augmented reality, internet-of-things and 3D printing.
- The advantages include productivity and reduced errors, the disadvantages include the cost and staff training.

Application File Types & Licences

- Your choice of application file types can define what software you must continue to use. It can also affect the features you can access and the file size.
- Application files types include:Software licences define how software can be redistributed and used.DOCX, DOC & RTF for word processing.
- XLSX, XLS & CSV for spreadsheets.
- PPT & PPTX for presentations. PDF can also be used for presentations & other applications.
- ACCDB & MDB for databases.
- Open source software allows you to both use the software and access to view & modify the source code.
- This has simpler licensing, you can alter the source code to adapt it to your needs, there are more regular updates and there is less "tie-in" to the software. However the software can be abandoned, maintaining the updates can be difficult, there is usually no professional support and code flaws can be identified & exploited easier.
- Proprietary software allows you to use the software but retains intellectual property rights so you cannot view, modify & redistribute the source code.
- It comes with the rights and expectations for the software to be maintained, it is usually simpler to update the software, there is usually good professional support and it often has better usability. However, licensing is often more complicated, the program can't be adapted to your needs updates can often take a long time to arrive and it can be difficult to transfer software.

- There are ten major factors to consider when choosing digital technology.
- User experience is about the feeling a person gets when making use of a device. Notable factors here include ease of use, performance, availability & accessibility.
- User needs are about what actual tasks the user wants to perform using the IT system.
- The specification is the list of components required of a computer system in order to allow users to run the software they need and perform their tasks.
- Compatibility is about whether the IT system can communicate with other devices you are using with it.
- Connectivity is about how a device can connect to a network, such as a LAN or the Internet.
- Cost is how much purchasing and running a device will cost you or your business.
- Efficiency is about how effectively tasks can be completed by the digital technology with as little wastage of resources.
- Implementation is about the time involved with putting a new system into effect. Notable factors here include timescales, testing & migration.
- Productivity is about how quickly tasks can be completed when making use of an IT system.
- Security is about how safe a device is from security threats, such as hackers &

Factors Affecting Choice of IT System

Wired Methods of Connecting Devices

- USB is a connector that is very commonly used with peripheral devices. It has fast transfer speeds, can connect multiple devices, provides power and is very compatible with computers. However, it does have a relatively short range.
- SATA is a connector that is most commonly used with internal storage devices but can work with external ones. It is very fast and very compatible with computer systems. However, it has a short range and doesn't supply power.
- VGA is a connector that is used with display devices. It is compatible with older devices and has built-in locking mechanisms. However the signal can degrade easily, it cannot achieve a very high resolution and doesn't include an audio signal.
- HDMI is another connector that is used with display devices. It is capable of excellent resolutions and transmits an audio signal too. However, it doesn't have a locking mechanism.
- Ethernet cable is used to transmit data between IT systems, often in a local area network. It is very reliable, has a good range and is very compatible with computers. It does offer limited mobility, is often not compatible with mobile devices and cannot transmit data over very long distances.
- Fibre optic cable is a method of transmitting data between IT systems that is commonly seen used as part of the telephone network. It has excellent transfer speeds & range and also is very secure. However, it is very expe

- Infrared is a wireless connection that is commonly used with remote controls. It was also commonly used with peripheral devices like wireless mice & keyboard, but not as much anymore. It has a low susceptibility to interference. However, it is short ranged, requires line of sight and is slow.
- Bluetooth is a wireless connection that is commonly used with peripheral devices like wireless mice & keyboards. It's also used to transfer data between two IT systems and to share a mobile broadband connection. It is easy to connect, has a low susceptibility to interference and has a low power consumption. However, it is also relatively slow and not very secure.
- WiFi is a wireless connection that is used to access the internet, create a wireless LAN and to connect to some peripherals such as printers. It is relatively fast and long ranged and has a low installation cost. However, it can be complex to set up and insecure.
- Mobile broadband is a mobile connection that is used with mobile devices to access the internet on the go. It is widely available wherever you are and is very easy to connect to. However, it is expensive and is quite a bit slower than WiFi connections.

Wireless Methods of Connecting Devices

Types of Networks

A Personal Area Network (PAN) is a network within the range of a single person.It is commonly created wirelessly using Bluetooth or wired using USB.
It is used to connect digital devices together, such as to sync files/emails/calendars between devices or transmit data with wearable devices like a headset.
It can reduce cabling, automatically sync data between devices & is secure for transferring data.
A Local Area Network (LAN) is a network that spans a relatively small geographical area, usually a single building or site.It is commonly created using ethernet cables, or WiFi for a wireless LAN.
It is used to allow computers to share resources, such as an internet connection, a printer or access to files.
It lets you share peripherals, access files flexibly and centrally manage computers.
A Wide Area Network (WAN) is a network that spans a large geographical area, such as an entire country or the whole world.It is commonly created using dedicated network lines rented from a telecommunications provider, but can also run over the public internet using a VPN.
It is used to transmit data securely between different locations in a business, such as confidential documents or emails.
It is secure, files can be accessed from across different business offices and is often very fast.

A Virtual Private Network (VPN) is a private network that runs across a public network, namely, the internet.
It is commonly created using an encrypted connection between computers.
It is used to transmit data securely between different locations without the cost of a dedicated private

- There are ten major factors to consider when choosing digital technology:User experience is about the feeling a person gets when making use of the network. Notable factors here include ease of use, performance, availability & accessibility.
- User needs are about what actual tasks the user wants to perform using the network.
- The specification is the specific requirements of the network in order to allow users to perform their tasks.
- Connectivity is about how the network can be connected to by devices.
- Cost is how much purchasing and running the network will cost you or your business.
- Efficiency is about how effectively tasks can be completed when using a network with as little wastage of resources.
- Compatibility is about whether the network can communicate with the devices you are using with it.
- Implementation is about the time involved with putting a new network into effect. Notable factors here include timescales, testing & downtime.
- Productivity is about how quickly tasks can be completed when making use of the network.
- Security is about how safe the network is from security threats; work files remotely, is cheaper than a WAN and is secure.
- The performance of a network is heavily affected by its components. For WAN.

Factors Affecting Choice of Network

19 of 43

There are ten major factors to consider when choos

20 of 43

- A protocol is a set of rules that defines a method for transmitting data between different devices over a network.
- Email protocols include SMTP for sending emails and POP3 or IMAP for receiving them.
- Voice & Video Calls over Internet applications use a variety of different protocols. SIP is a common protocol for establishing a connection while RTP is used for transmitting the data and RTCP is used for providing feedback on the quality of data delivery.
- Web pages commonly use HTTP for accessing web pages stored on a server. HTTPS is a version of HTTP that uses encryption for security. FTP is commonly used for uploading web pages onto a server.
- Secure Payment Systems rely on HTTPS for transmitting bank details from the user's computer to the only retailer in a secure manner. SET and 3D Secure are both specific secure payment protocols used to perform an online transaction securely.

- When transmitting data over a network you are vulnerable to eavesdroppers.
- Sniffing uses packet sniffers to inspect data not meant for your computer in order to gain unauthorised access.
- Spoofing is where a computer pretends to be another computer in order to gain unauthorised access and can harm network performance through DoS attacks.
- Wired transmission methods are generally more secure than wireless as a hacker would need to be physically near the cable.
- Firewalls help prevent unauthorised access to data by monitoring traffic and blocking anything suspicious.
- Encryption helps to prevent unauthorised access by making data unreadable until it has been decrypted.

Data Transmission Security Issues

Bandwidth, Latency & Compression

The bandwidth of a network is the amount of data that can be transferred from one computer to another in a given period of time.

The latency of a network is a measure of the time it takes for a data packet to transfer over a network.

Online gaming requires a low latency due to the quick response time needed, however it doesn't need a large bandwidth.

Online streaming requires a large bandwidth due to the amount of data that is transferred, however it doesn't need a low latency.

Compression is used to reduce the size of files. This is helpful in networking as it means we need less bandwidth to transfer a file.

Lossy compression permanently deletes certain bits of data to reduce file size. It is commonly used in video, audio & image compression.

Lossless compression uses algorithms to pack the data into less space. It is commonly used in document compression.

Lossy compression reduces the quality of a file and cannot be decompressed back to its original quality. Lossless compression cannot reduce the file size as much as lossy.

Hardware CODECs are used to encode analogue data into digital data. It will then decode the digital data into an analogue form.

Software CODECs are used with audio and video to compress the data so that it used transmitted over a network.

A downside to CODECs is that there can be compatibility issues due to the variety

Using Online Systems

- With cloud storage, your data is stored remotely on servers.
- This is used in our personal lives for portable data storage uses syncing files across multiple devices & sharing files with others.
- It is used in our professional lives for remote data backups and remote working.
- Cloud Computing refers to accessing the resources (processing, storage, etc) of a server over the internet.
- We use this in our personal lives for accessing software applications across multiple devices at a low cost.
- It is used in our professional lives for accessing software with low maintenance needs and to support cloud computing.
- The benefit of using cloud storage & computing to individuals is that the software can be accessed flexibly, data can be synced between multiple devices and theft of equipment won't lose your data.
- The drawback of using cloud storage & computing to individuals is that there can be security concerns and it requires a stable, fast internet connection.
- The benefit of using cloud storage & computing to businesses is that there are reduced upfront costs, access can be flexible to your business needs and less IT staff are required for maintenance.
- The drawback of using cloud storage & computing to business is that security can be a concern and productivity is damaged if the network/internet goes down.

Remote Working & Choosing Online Systems

- Virtual private networks are used in business to allow a user to connect to their work LAN while working remotely.
- Remote desktop technologies allow a user to access their work desktop from outside the business offices.
- The factors to consider when choosing an online system are security, cost, ease of use, features & connectivity.
- Security is important as data being transmitted over a network can be intercepted. Features such as using SSL help to protect data by encrypting it.
- Cost is a factor as most online systems will charge a subscription fee for organisations to access their services. This can vary from different companies and is often flexible to a businesses needs.
- Ease of use is important as if employees find it difficult to use the online systems they will avoid them. Good accessibility for different devices and users with individual needs is important too.
- The features offered by an online system provider is likely the most important factor. To perform our business functions we need the online system to have certain features.
- Connectivity is a factor because online systems require fast, reliable broadband connections.

- Social Media websites, such as Facebook, allow you to visit (or Like) pages dedicated to topics of interest.
- Blogs & Microblogs are websites where you can write posts about news and opinion on a topic of interest. Vlogs are similar but are done in video form, rather than written posts.
- Wikis are a website where the content is created by a community of users who share a common interest.
- Chatrooms are websites that allow for online communities to communicate via short text messages on a shared topic of interest.
- Instant Messaging allows you to have a text-based, real-time conversation between two people, or a small group.
- Podcasts are audio or video files that are shared over the internet to share information on a particular topic.
- Forums are websites where users can post messages which can then be responded to by other forum users to take part in a discussion

Implications of Online Communities 1

- A good user experience is required to keep users on your site. They expect it to be easy to use to perform actions, it should have good performance, available to them to use and accessible to any individual disabilities.
- People use online communities that meet their personal reasons for accessing it. This might be to access the latest news or keep in touch with friends. They also may have individual needs for accessibility for disabled people or for certain devices or connections. Without that, they will look at other online communities.
- It is free to use for individuals, but advertising must be accepted in its place based on profile information. This can lead to impulse purchases. You also need to pay for an internet connection.
- Personal information could be public and misused. Personal information or photos could be used for identity fraud or cyberbullying for example. Employees may see posts and this could affect employment.
- User profiles can be hacked and personal data stolen and misused. Not all sites implement the best security procedures and this might lead to bank fraud, identity fraud, cyber bullying etc.

- Employee & Customer Experience – Sites used should be easy to use, quick to load, available anywhere and accessible to employees and customers with disabilities.
- Customer Needs – Online communities must respond to customer needs effectively and timely.
- Cost – Organisations may need to hire and train staff and might want to pay to boost awareness of their online community.
- Implementation – It will take time to implement an online community and will require extensive testing.
- Replacement or Integration with Current Systems – Data may need to be transferred and systems may need to be able to communicate with each other. This may cause downtime.
- Productivity – Productivity can be improved by aiding communication but can lead to employees being distracted from their jobs.
- Working Practices – New guidelines will be needed to ensure the correct use of online communities by employees.
- Security – Businesses should protect themselves from having their accounts hacked and misused.

Implications of Online Communities 2

Implication of Threats

- Malware includes things like viruses, worms, trojans and spyware. This can corrupt or delete data which will be expensive to recover and can lead to data being stolen for bank fraud purposes.
- Hackers are someone who gains unauthorised access to a computer system. Malicious hackers do so to misuse data, such as delete it, alter it or steal it for blackmail, bank fraud and identity fraud.
- Phishing is where emails are sent purporting to be a reputable company, but in fact, has been sent by a malicious user for the purpose of gaining personal or financial information in order to commit bank or identity fraud.
- Accidental damage is where IT systems or data are harmed through human error, such as dropping a device or accidentally overwriting important files. This can be costly, as you need to recover or re-enter the data that has been lost and replace harmed equipment.

- File permission means that you can set who can access files and what they can do with them. There are three main file permission types: read-only, read/write and full control.
- Access levels control what software, data and services a user can access. The highest level is administrator access.
- Backups involve taking a copy of the data and storing it in a secondary location. This is normally in a different building, called a remote backup. There are three main types of backup: full, incremental & differential.
- Physical access controls prevent unauthorised users from gaining access to our IT systems. Examples of physical access controls include access cards, keypad access control, biometric access control & electronic locks.
- Digital certificates are used to authenticate a user as the owner of a public key so they can use public key encryption. Two key parts of a digital certificate are the signature and the public key.
- Protocols are a set of rules that defines a method for transmitting data between different devices over a network. Security protocols that are used include SSL and TLS. These allow us to send data securely over the internet using encryption.

Protecting Data Techniques

Protecting Data Tools

Anti-virus software is a utility program that is used to prevent malicious software from infecting your computer or detect and remove malicious software that has already infected your computer.
Some of its implications are that it must be regularly maintained and updated, it doesn't offer complete protection and it can slow performance.
Firewalls are either a hardware device or a utility program that monitors incoming and outgoing network traffic and blocks any traffic that it deems suspicious.
Some of its implications are that it can diminish network performance, impair productivity and cannot prevent internal attacks.
Encryption is where data is converted into an encoded form so as to prevent unauthorised access.
Stored data use symmetric encryption. This uses the same key to both encrypt and decrypt the data.
Some of its implications are that if you lost the encryption key you cannot recover the data and the sharing of the encryption key can compromise security so it is no use for encrypting data during transmission.
Data during transmission uses asymmetric encryption. This uses different keys to encrypt and decrypt the data.
An implication of asymmetric encryption is that it can affect the performance of your device during encryption/decryption.
Legislation has been implemented to protect data and IT systems. These include the Data Protection Act & the Computer Misuse Act.
Professional bodies and the Information Commissioner's Office produce codes of guidelines to help ensure businesses follow best practice and comply with relevant laws.

Anti-virus software is a utility program that is used to prevent malicious software from infecting your computer or detect and remove malicious software that has already infected your computer.
Some of its implications are that it must be regularly maintained and updated, it doesn't offer complete protection and it can slow performance.
Firewalls are either a hardware device or a utility program that monitors incoming and outgoing network traffic and blocks any traffic that it deems suspicious.
Some of its implications are that it can diminish network performance, impair productivity and cannot prevent internal attacks.
Encryption is where data is converted into an encoded form so as to prevent unauthorised access.
Stored data use symmetric encryption. This uses the same key to both encrypt and decrypt the data.
Some of its implications are that if you lost the encryption key you cannot recover the data and the sharing of the encryption key can compromise security so it is no use for encrypting data during transmission.
Data during transmission uses asymmetric encryption. This uses different keys to encrypt and decrypt the data.
An implication of asymmetric encryption is that it can affect the performance of your device during encryption/decryption.
Legislation has been implemented to protect data and IT systems. These include the Data Protection Act & the Computer Misuse Act.
Professional bodies and the Information Commissioner's Office produce codes of guidelines to help ensure businesses follow best practice and comply with relevant laws.

Protecting Data Tools

Features of Online Services

Retail services, such as e-tailers and online auctions, offer customers a wide choice, easy price comparison and easy access. However, you could be sold products that are never delivered and the lack of regulation can lead to dangerous products being sold.

Financial services, such as online banking, loan and trading sites, allow great flexibility in managing finances and total awareness of your financial situation. However, there are security concerns and some services may operate in countries without regulation.

Education & training services, such as distance learning qualification sites and MOOCs, gives access to a wide range of courses and allows you to learn in your own time. However, many online qualifications are not accredited and learners must have good self-motiviation.

News & information services, such as news sites, traffic reports and weather reports, make it easier to keep informed and make it easier to plan events & trips. However, it can be difficult to identify genuine information and news can be released too soon.

Entertainment & leisure services, such as video/music streaming and online gaming, give access to a range of entertainment, we can access more flexible and online gaming allows us to play with others around the world. However, it can lead to children accessing inappropriate content and can distract us in our lives.

Productivity services, such as cloud computing, video conferencing and remote desktop software, allow employees to work more flexibly and collaborate easier. However, it makes a company reliant on their internet connection and cause work to creep into our personal lives.

Booking system services, such as holiday, cinema & train booking, allow custome

reduces the need for admin staff and allows us to book from home 24/7. However, there are security online payments.

- Transactional data is the data collected from a sale or purchase.
- It is used for keeping purchase records, tracking delivery and identifying customer habits.
- Transaction data could be hacked and the data misused. There are also concerns over the privacy of individuals.
- Targeted marketing is all about advertising products to the customers who are most likely to purchase the product.
- It is used for customising web pages to user's interests, search engine advertising & social media advertising.
- Targeted marketing can lead to impulse purchases and can take advantage of vulnerable people. It also brings concerns over privacy.
- Collaborative working is where multiple individuals can work together in real-time over the internet.
- It is used when we share & work together on documents using cloud storage and computing, when teleworking from home and when talking with colleagues using VoIP and video conferencing.
- There need to be careful restrictions to prevent users from overwriting each other's work, security can be a concern and business productivity can be harmed should the internet connection go down.

Uses of Online Services

Features of IT Systems 1

- Stock control uses IT systems to monitor and control their stock and can allow the implementation of automated and JIT stock control.
- This simplifies tracking stock ensuring the business won't run out of stock and also reduces the need for admin staff. However, stock control systems can be expensive to implement and theft can lead to the business running out of stock.
- Data logging uses IT systems through the use of sensors to monitor a process and automatically log the data.
- This is far more accurate and is better for tracking changes over time to spot trends & patterns. However, if your connectivity goes down then readings will be missed and if not calibrated correctly the sensors will record inaccurate data.
- Data analysis is done using IT systems to spot patterns and trends and make future predictions.
- This makes it easier to spot trends & patterns and allows you to convert the data into different formats easily. However, if incorrect data is provided it will produce incorrect results and data could be stolen by hackers.
- General office tasks use IT systems to produce documents, writeup notes, manage finances, communicate and schedule appointments.
- This allows for tasks to be completed more efficiently and with allows staff to perform a wider range of tasks. However, employees need greater technical skills and business will need to maintain IT support staff.

Features of IT Systems 2

- Creative tasks use IT systems for things like CAD, graphics design and music/film editing.
- This makes it easier to edit and change creative work and makes it easier to share it. However, it requires a large storage capacity and has lead to issues with piracy.
- Advertising uses IT systems through the use of online advertising, print advertising & video adverts.
- This allows businesses to target customers better and viral campaigns can gain wide recognition at low cost. However, it has seen problems with spam and phishing emails.
- Manufacturing uses IT systems for Computer-Aided Manufacturing of products like car parts and clothing.
- This allows for a more consistent and higher standard of product and saves money due to reduced staff salaries. However, it does lead to job redundancies and does have a high initial cost to implement.
- Security uses IT systems such as door/window and motion sensors connected to an alarm, security cameras & RFID sensors to detect theft.
- This means the business needs less security staff and generally improves business/home security. However, it does lead to privacy concerns and can give a false sense of security.

Impact of IT Systems

Poor user experience can impact on employee productivity. Such as if it is difficult to use, has poor performance, is not easily available or is not accessible to those with disabilities.

IT systems can help a business meet employee needs by making their jobs easier, more efficient and safer. They can help a business meet customer needs by improving communication and tracking service quality.

There is often a high initial cost for purchasing new IT systems and training staff to use them. However, they usually save money in the long run by allowing the business to run with less staff.

The implementation of an IT system takes time due to lead times for delivery, testing and downtime for installation. This can leave the business without a functioning system costing them business.

When replacing or integrating an IT system there is usually downtime as well as a period of teething problems. This can cost the business money and harm its reputation.

IT systems support productivity by allowing businesses to function longer hours and saving time. However, they can lead to distracting employees and poor productivity if IT systems stop working.

IT systems have changed working practices. We can now work more flexibly, such as at home, but can often find expectations of being available 24/7.

IT systems have changed jobs so employees need better technical skills. There also needs ongoing training for new systems which is expensive for the business.

User support is required for IT systems. If it isn't in place employees will not be productive and may not use the system at all. Having user support available is expensive for the business.

Businesses need to keep themselves secure from threats to IT systems. This is exp
don't they could be fined under the data protection act.

- Primary data is data that has been gathered through original research done by the organisation or individual.
- Benefits of primary data are that it is more up-to-date, it is more relevant and it is more reliable.
- Secondary data is data that has been gathered by someone other than the user of the data.
- Benefits of secondary data are that it is cheaper, quicker to obtain and not affected by the organisation's bias.
- Data must be reliable to be useful. Reliable data is complete and accurate. Secondary data should always come from a trustworthy source.
- There are three methods of completing a survey.
  - Questionnaires involve a set of questions, normally in a closed question format, used to gain information for statistical analysis, or personal information from respondents.
  - Focus groups involve a group of people being asked questions on a particular topic.
  - Interviews are a one-to-one meeting where an interviewer asks questions to a single respondent in order to gather information.

Data Sources

Processing & Presenting Data

It is extremely important to ensure data accuracy as computers don't have the common sense to spot errors and so if bad data is entered bad results are outputted (GIGO).
We can help ensure data accuracy through the use of validation and verification.
Validation is a check to ensure data is sensible and reasonable. E.g. a length check or type check.
Verification is a check to ensure data matches the original source. E.g. a proofreading check or double entry check.
Data is organised into a database and we use queries to extract and sort data.
Extracting can be performed by choosing specific fields and using filters to select data that meet specific criteria.
Sorting can organise data by any retrieved field in ascending or descending order.
Numerical modelling is where mathematical calculations are used to simulate a real-life system.
Data modelling is a process used to plan the structure of a database to ensure that data is stored in the most organised and efficient manner.
Data can be presented in tabular or graphical format.
Tabular presentation is a text presentation of data within a table. This is used where precise data and detail is required.
Graphical presentation is where data is presented using a chart or s
of diagram. This is used where ease of interpretation and spotting trends is required.

An easy to use interface must have clear navigation, good labelling and simplified input methods.
An accessible interface should consider the individual needs of users with disabilities. Such as using a clear and simple interface, high contrast colour schemes and support changing of sizes.
Error reduction in a user interface can be achieved through validation/verification checks, input masks and warning messages.
An intuitive interface is easy to use even with little training. This can be achieved by making it easy to use and keeping the interface similar to paper forms or previous systems.
Functionality in a user interface is about allowing users to be able to perform the required tasks they need from the system.
The performance of a user interface can be improved by ensuring that tasks can be completed in few steps, it's easy to navigate and reducing the likelihood of errors arising.
Compatibility affects the user interface. A highly compatible interface will allow data to be inputted to and from different IT systems.

Data Collection User Interfaces

Moral & Ethical Factors 1

The growth of information technology has caused an increase in landfill trash (technotrash). It also consumes materials, power, chemicals & water to produce technology. We also use more power to run our technology systems. This is all harming the environment.

Many poorer people have very limited access, or no access at all, to information technology. This is impacting on the poor, especially young people, as they cannot use these for things like education.

Poor online behaviour is a relatively common issue. Acting poorly online can affect your employment and can lead to legal problems. Being the victim to abuse online can lead to suicide. The rules for good online behaviour is known as netiquette.

Information technology is increasing globalisation, where the world is becoming more interconnected and integrated. This can lead to outsourcing which affects employment. It is also seen to affect cultures, spread disease and increases pollution.

We use information technology to freely express views and opinions. However offensive opinions are often censored to prevent causing offence. Some see this as a violation of their freedom of speech.

Most businesses have acceptable use policies to govern how employees use their IT systems. This covers things like sites they can visit, the language they can use and sharing copyright material. This can lead to termination of contract if breached.

Health & Safety concerns have grown with IT systems. RSI, eye strain and tripping hazards are just three examples. Businesses must make sure they take care this doesn't affect employees causing injury.
The downloading of copyright material without permission is a big problem with IT systems. It is costing people and businesses a lot of money where people access movies, images, music, etc. for free. This can cost people their livelihood.
The threat of computer misuses, such as hacking and viruses, is very real. While some attacks are just a nuisance, it can also be very serious, costing an organisation a lot of money which could cause them to go out of business.
Organisations and individuals must protect the data of others. If they do not then the people who have had their data stolen could be seriously harmed, such as having their identity stolen or money from their bank.
Privacy is a big concern. More and more information about us is appearing online. We often aren't even aware of this, such as when people share images of us. This information can be misused, such as with cyberbullying or identity fraud.
Organisations should make sure their IT systems are accessible to people with disabilities. This might involve installing adaptive technology. This is to stop them from discriminating against individuals which cause stress, upset and affect employment.

Moral & Ethical Factors 2

Data & User Protection Legislation

The Computer Misuse Act (1990) protects users against the theft and damage of the information they store using IT systems. There are different punishments depending on the crime, but could be as much as 10 years in jail and/or a large fine.
The Police and Justice Act 2006 (Computer Misuse) extended the Computer Misuse Act so that it covered Denial of Service Attacks as well as the making, supplying or obtaining anything which can be used in computer misuse offences.
The Data Protection Act (1998) protects the privacy of individuals by ensuring that their personal information is processed in an ethical manner. There are 8 principles that must be complied with. If in breach of the DPA then an organisation can be fined as much as £500,000.
The Copyright, Designs & Patents Act (1988) protect the creators of original works by giving them the right to control how these original works are used. This is usually punished through damages being paid, however, it can receive as much as 10 years jail time.
The Copyright (Computer Programs) Regulations (1992) extended the Copyright, Designs & Patents Act to ensure that computer programs are covered under copyright.
The Health and Safety (Display Screen Equipment) Regulations (1992) extended the Health & Safety at Work Act so that users of display screen equipment are not harmed in some way. Failure to comply with these regulations is normally punished through a fine, though imprisonment is also possible.
The Consumer Right Act (2015) brought together all existing consumer rights legislation into a single act. It also ensured digital content is covered by consumer rights for the first time. This gives consumers the right to repair, replacement or refunds should digital content be faulty. Consumers can also take busine
they not receive this.

Accessibility Legislation & Guidelines

- The Disability Discrimination Act (1995) was a piece of legislation designed to prevent businesses & government from discriminating against the disabled.
- The Disability Discrimination Act (2005) was a new version of the legislation that made substantial amendments to the original 1995 act.
- The Equality Act (2010) replaced the Disability Discrimination Act, along with 115 other pieces of legislation, including the Sex Discrimination Act, Equal Pay Act and Race Relations Act. It mostly carried through the provisions of the DDA but did make a number of changes.
- The British Standards Institute are an organisation who define national standards for best practice in a number of areas. As part of this, they have defined a wide range of standards such as the Web Accessibility Codes of Practice.
- The Open Accessibility Framework is a guideline for ensuring any IT system is accessible, whether it is desktop, mobile or web-based.
- The Web Content Accessibility Guidelines 1.0 and 2.0 define guidelines for making web applications accessible.