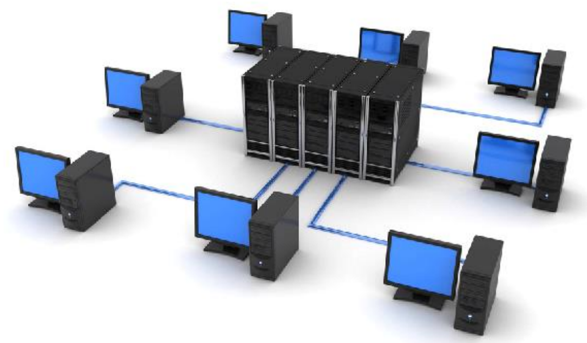
BTEC Tech Award

Digital Information Technology

Component 3 Revision

The Marlborough Science Academy
'shaping futures'

Networks



Traditional networks

These contain powerful computers called servers to run the network. They also have other PCs and devices like routers and hubs. They are all joined together with wires.

Good things: Fast and reliable.

Bad things: Expensive to set up. Harder to add new devices.

Ad-hoc networks

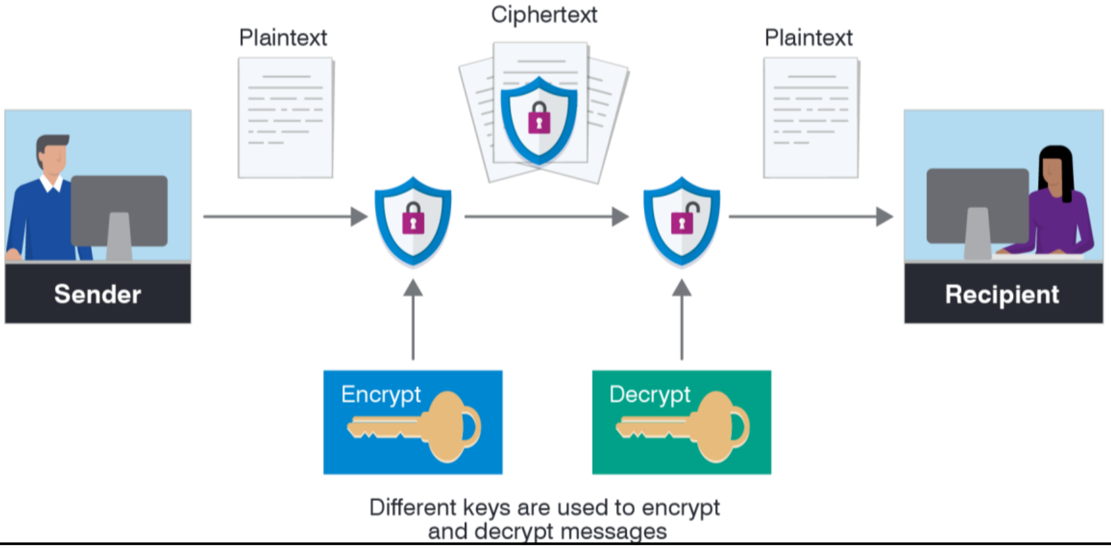
These are more flexible because it is easy to add devices as you need them. They usually use WiFi.

Good things: Easy to add new devices. Cheap to set up.

Bad things: Connections can be slow and unreliable. You need to be nearby.

At home, do you have a traditional or an ad-hoc network?

Encryption is when data is disguised using an encryption key. If somebody steals the data they will not be able to read it without the same key. WhatsApp encrypts all of your messages.



You must be careful when using **WiFi hotpots**.

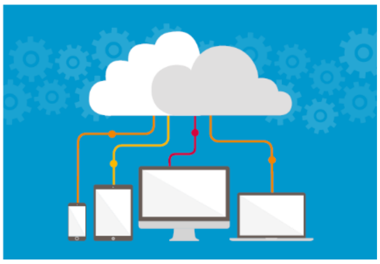
Many hotspots are **insecure**. This means other Users can intercept your data and can get your login details, bank account information, etc.

You can use your phone to make a personal hotspot. You can then **tether** (link) computers to your phone.

The Cloud

Important!

When we talk about ‘the cloud’, this does not mean **actual** clouds. It means services available to us over the Internet.



Cloud storage

You probably already use one of the services below to save images and other files on the Internet. These are all examples of cloud storage – you save on the internet, not your device.

Dropbox iCloud Google Drive

Benefits of cloud storage

You can access your files from anywhere with an Internet connection.

You don’t have to back things up – they do it for you.

It is **scalable** – this means you can buy more space if you need to.

Downside of cloud storage

You need an Internet connection to access your files.

Extra storage space can be expensive.

You have to trust the company to keep your data safe and secure.

Key term: Synchronisation

This is when cloud storage is used to make sure that two or more devices all have access to the same files. iTunes synchronises music on all your devices.

Online applications

An **application** is a software tool that you use. Applications like Microsoft Word have to be installed on your computer to use. Applications like Google Docs do not need to be installed – they are **online applications** which you use online through your web browser.

Benefits of online applications

You don’t need a computer with lots of memory because you don’t need to install the software.

You can **collaborate** (work on the same document at the same time) with somebody else anywhere in the world.

No need to install updates on your computer.

Downside of online applications

Online applications sometimes aren’t as powerful or have as many features as installed applications.

Some online applications have ongoing monthly costs.

You need access to the Internet to be able to use the software.

What do you think might be the advantages and disadvantages of editing a document at the same time as somebody else is working on the same document?

Selecting a platform

Desktop computer	Notebook	Tablet	Smartphone

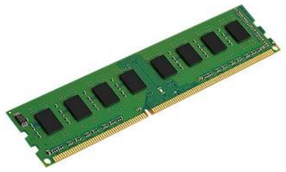
All of the platforms above can connect to cloud services. When selecting which device to buy or use you might think about…

Screen Size

Some services (such as graphics editing software) will need large screens.

Portability

How easy the device is to move. Some services need you to be able to move – can you imagine playing Pokémon Go on a notebook?



RAM

More RAM (Random Access Memory) is needed to run more powerful software.

Storage Capacity

If you need to save lots of files and install large software you will need more storage capacity.

Operating system

e.g. Windows, iOS, Android. Some services are only available on certain operating systems.

User Interface

Some services need touch screens, stylus, keyboard, voice control, etc.

Selecting cloud services

Imagine you need to decide between different cloud services available. For example, you might be selecting an online service for storing files or an online service for making spreadsheets. What will you need to think about?

Cost

Many online services start free, but can become expensive e.g. if you need to increase your storage space.

Security

As your data will be stored in the cloud, how does the service make sure your data can't be stolen or lost?

Storage space

If you need to store data and files online, how much space do the cloud services give you?

Ease of use

A service would be no use if the software is too difficult to use. Expert users may want more complex tools.

Downtime

Downtime is a period when a cloud service is not available to the users. This might be because they are updating systems or it might be because something is broken. For some organisations it would not be acceptable to have **any** downtime, e.g. air traffic control must always be working!

Collaboration

Collaboration means to work with other people.

Technology is allowing people to collaborate in ways that were never possible before. You need to know some features and benefits of collaborative technology.

Benefits of collaborative technologies

Team flexibility
Teams can work together even if they are in different locations, countries or time zones.

24/7/365
Cloud services meant people can work together any time of the day, any day of the year.

Less travel
People do not need to travel to work with others. This saves time and is better for the environment and for people with disabilities.

Inclusivity
People get the chance to work with people of different ages, backgrounds and cultures.

Features of collaborative technologies

Chat tools
You can send and share messages to people you are working with. This is faster than using email.

Video conference
You can have face-to-face meeting with people in different locations using webcams.

Schedules
Teams can share a calendar with key dates showing deadlines things need to be finished by.

To-do lists
Lists of tasks showing what individuals or teams have completed and what still needs to be done.

Monitoring
Team leaders and managers can track progress and monitor the work of their teams

File sharing
Easily share files and folders with other team members. Even work on the same file at the same time.

Key term: Version Control
Version control records changes to documents and files over time so that all versions can be recalled if needed.

WHAT'S THIS CUP OF USB DRIVES?
AH, THAT'S HOW I VERSION-CONTROL MY FILES...
TYPE
TYPE
TYPE
STAN'S DESK!
IT'S BRILLANT REALLY. JUST MAKE A NEW COPY ON A NEW ONE EVERYDAY.
WHAT HAPPENS WHEN YOUR CUP FILLS UP?
EASY! I DUMP THEM IN HERE!
USB

On this page we have thought about the features and benefits of working collaboratively using technology. Can you think of any possible disadvantages?

Accessibility

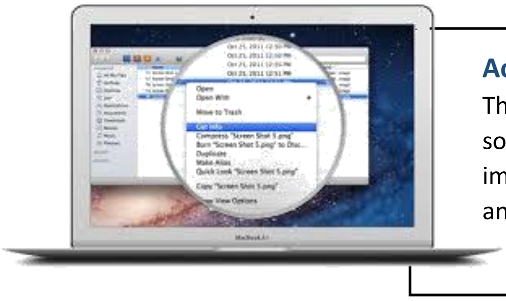
Computer systems must be designed so that they are easy for everybody to use, even if they have a disability. Disabilities might include hearing issues, eyesight problems (e.g. blindness), motor problems (problems to do with movement) or learning difficulties. Accessibility is whether or not a system can be used by people with different needs.

Accessibility issues to consider

Interface design

The interface design is what we see when we use a digital tool. They should be designed to be as easy to use as possible. Good interfaces should be **responsive** – this means they will change their layout on different size screens (smartphone screens should look different to desktop computer screens).

ILLUSTRATED BY SEGUE TECHNOLOGIES

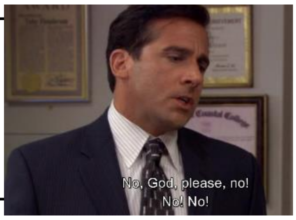


Accessibility features for visual impairment

Think carefully about choice of colours to make sure they don't clash. Remember some people are colour blind so your colour combinations must not make it impossible for them to read text. Screen magnifiers can help people who need text and images to be made bigger. Text to speech can be used to read information to blind people. Add 'ALT' (alternative) text descriptions to pictures to help blind people.

Accessibility features for hearing impairment

Interface features should not rely on people hearing instructions. Deaf people would not receive these instructions. If video and audio needs to be included, then users should be able to access subtitles so that they can read what they cannot hear.



Accessibility features for cognitive needs

People with cognitive needs may need help and extra time to understand things. They might be provided with the option to have text read to them. Spell check might be built in to help avoid mistakes. Keep layout of screens consistent (don't keep moving things around).

Inclusivity

Inclusivity means making sure that everybody has a chance to be involved and take part.

Businesses can use technology to ensure that all employees have a chance to take part in work and to contribute to the business. This might include:

- Allowing somebody recovering from an operation to work from home.
- Allowing people to work flexible hours (e.g. starting later).
- Using technology to convert information into a range of languages to allow people to read information in their chosen language.

Threats to data

IT systems are often under attack. Attacks can come from inside (internal) or outside (external) an organisation.

Internal threats

Internet downloads

Staff might download software from the internet which have a virus. When they run this software it can infect the IT system and cause problems.

Use of USB sticks

Staff might bring USB sticks which are infected with viruses. Some staff might steal company data by copying it onto USB sticks.

Stealing or leaking data

Staff might steal data and give it to a rival company (this is called ‘leaking’). They might do this for money or if they are unhappy with the company.

Mistakes by staff

Staff might accidentally cause damage to an IT system. They might be careless with usernames and passwords or leave computers logged on when they go.

Unsecured devices

Staff might use unsecured devices (e.g. their own smartphones) to access company data. If the devices are hacked or stolen criminals might get the data.

External threats

Hacking

Hacking is when somebody gains access to a system without permission. They can do this for personal gain, e.g. by stealing data or money.

Phishing

This is where people send a fake email which is aimed at tricking you into providing personal details like passwords, account details, etc.

Denial of service

A denial of service attack is where somebody sends a huge amount of data to a network to make it crash – like when websites crash when they are busy.

Pharming

Where somebody sets up a fake website which looks real but which collects usernames and passwords which criminals can then use.

Man-in-the-middle

An attack where messages between two devices are intercepted by criminals who might then be able to use the information in the messages.

Reasons people carry out attacks on IT systems

- For money.
- By mistake.
- Out of boredom.
- Angry at the organisation.
- To prove they can do it.

Key terms

Social engineering

Getting users to share sensitive information through tricking them. An example would be criminals phoning you pretending to be your bank.

Ransomware

A type of malicious software which blocks you from getting access to a computer system until a sum of money is paid.

Security breach

When security to protect an IT system fails and data is lost or stolen. This could be by accident or by deliberate attack.

Productivity

A measure of effectiveness – how long it takes an employee to complete a task or a series of tasks. This can be reduced by IT security breaches.

Protecting data

Now that we understand there are risks to the data kept by companies, what can they do to keep the data safe?

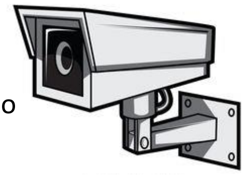
Controlling who gets access

Swipe cards

Doors stay locked unless you have a swipe card to unlock the door. Unlike normal keys, cards can be cancelled if lost.

CCTV

Does not stop data being stolen but acts as a deterrent (makes people less likely to try to break in) and records break-ins.



Physical locks

Prevent devices being stolen by locking them in place using locks with steel cables. The downside is you can't move them.

Passwords

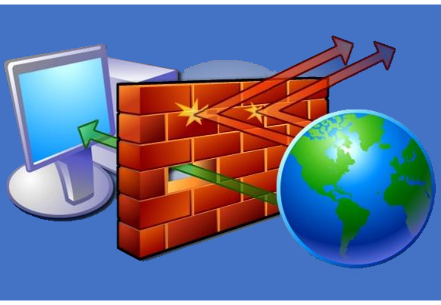
You can add passwords to rooms and to devices. Passwords can be lost, forgotten or hacked using specialist software.

Biometrics

This is when we use our body to gain access to something, e.g. through scans of finger prints, eyes or faces.

User access levels

Users are only given access to data and tools that they need. This limits the number of people who can cause problems.



Key Term: Firewall

A firewall controls the data coming into or out of a network. They can be either software or hardware. They can stop hackers accessing a network and stealing data. They can also stop staff getting onto websites you don't want them to use (in the same way as the school firewall stops you getting on game sites and YouTube.

Focus: Anti-virus software

Malicious software is software which tries to damage a computer system in some way. Most viruses get into a computer system when the user opens an infected email attachment or visits a 'dodgy' website. Anti-virus software scans a computer to try to find and remove any malicious software. It is important to keep anti-virus software updated.

You need to know the different types of malicious software (virus)…

Worms

A worm is a small computer programs that can spread to other programs.

Trojans

These look like useful tools you might want to install and use, but they are actually viruses in disguise. Once installed they can infect your system.

Rootkit

A collection of programs which help a hacker to gain access to a computer system.

Spyware

Software installed on a computer which watches what a user does and sends information about things like usernames and passwords to criminals.

IT Policies

A policy is a set of rules and guidelines that is written by an organisation which must be followed by people working in the organisation. You need to know about two policies....

Security policies

A security policy will be written and reviewed by the IT manager as he / she will have the best knowledge for protecting the IT system. The IT team will make sure that the organisation is doing everything in the security policy.

Things to include in a security policy:

Data Security: How the organisation will make sure that data is safe and cannot be lost, damaged or stolen (e.g. with encryption of data and regular backups).

System security: How the organisation keeps systems secure and keeps viruses and hackers out (e.g. with firewalls, antivirus software and secure passwords).

Disaster recovery: A disaster might be a flood, fire, virus or theft of data. The security policy should plan for this by thinking about:

- Potential risks and how to avoid them
- What staff should do in the event of an IT disaster
- Making sure backups work and they can recover data

Acceptable use policies

An Acceptable Use Policy (AUP) explains the rules the users of a computer network must follow. This will have many of the same rules included in our school technology agreement that you sign up to each year. An AUP might include…

Rules about user passwords

Users must not share their passwords with anybody, must make sure they are complex and must change them often.

Rules about storage devices

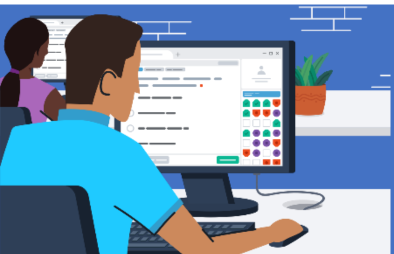
Many organisations ban people from using their own storage devices like USB sticks in case they bring in viruses on them, copy data they shouldn't, or lose the USB with data on it.

Rules about software

Most users will not be allowed to install software on the network without getting permission and having it checked first (in case it is malware and causes a problem).

Rules about internet and email

Users will be told to think carefully about opening email attachments and the websites they visit in case they add a virus to the network. They should only use appropriate websites.



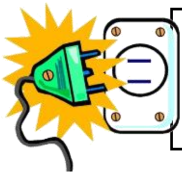
Key Term: Software audit

A software audit is when you make a list of all the software installed on your network. This includes the name of the software, the version, the date it was installed, and which computers it has been installed on.

Environment

Technology can have a very negative impact on the environment. We need to think carefully about how we used technology to minimise our impact.

Negative impacts



Electricity Generation

Digital devices use electricity. Creating this electricity can damage the environment by releasing greenhouses gases and leading to climate change.

Waste materials

Lots of digital devices, hardware and batteries end up in landfill sites. Much of the materials cannot be recycled. Some waste will leak chemicals into the environment and poison plants and animals.

Raw materials

Making digital devices uses raw materials which are finite (they will eventually run out). Some of these materials (like silicon) are very rare. The environment can also be damaged by mining the materials.

Steps to protect the environment

Reuse and recycle

Wherever possible, technology should be reused or recycled rather than thrown away. Some charities collect old mobile phones and send them to remote parts of poor countries to help people there.

Reduce electricity usage

You should turn off devices when they are not being used. You can set devices to turn off automatically after a period of inactivity. You can also use power save settings like reducing brightness.

Reduce use of consumables

Consumables are things like paper and printer toner which can run out and you need to replace. You should try to avoid printing things out unless you really need to. Files can be sent by email rather than being printed and sent by post.

Upgrade rather than replace

If possible, you should try to upgrade computers to make them faster rather than getting rid of them and buying new ones. Computers can be made faster by adding more RAM.

How can technology help the environment?

- ✓ People can work from home so less car journeys are needed.
- ✓ You can send documents electronically rather than on paper.
- ✓ We can read books on digital devices rather than on paper.