CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A1 Modern Technologies – Ad Hoc Networks

Key Vocabulary	
Bluetooth	A short range technology (10 metres or less) that can connect multiple devices. e.g. mobile phones & speakers
Ad hoc Network	A wireless network that does not rely on fixed hardware such as routers in wired networks.
Personal Area Network	Used for data communication between devices.
Tethering	Where a smartphone acts as an access point, allowing other devices to connect to it to share its mobile broadband connection to the internet.
Personal hotspot	Using a phone's internet connectivity to access the internet from the laptop.
PIN	Acronym meeting Personal Identification Number
Encrypted	Information or data has been converted to a type of code that cannot be understood without a translation key.
USB	Universal Serial Bus. A standard for connection sockets on computers, connecting devices such as mice, keyboards, printers, external hard drives, etc.
Insecure	A connection where data maybe intercepted by other users.
Streaming	Data is sent to your device in a continuous flow when connected to the internet.

Traditional vs ad hoc networks

Traditional networks are made up of several PCs, routers and other devices that are connected using cables and wires. 	**Ad hoc networks** are networks that do not require wires or cables, Modern technology has made it possible for organisations to connect devices when they are needed. 

Benefits of ad hoc	Drawbacks of ad hoc
√ They are scalable	x They are less secure.
√ They are flexible	x They have a reduced speed.
√ They require limited setup.	x The network can become unorganised.

Examples of ad hoc networks:

- PAN
- Open Wi-Fi
- Tethering or Personal Hotspot

Issues affecting availability:

- Rural vs city locations
- Developed vs developing countries
- Available infrastructure
- Mobile network coverage
- Blackspots

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A1 Modern Technologies – Features of Cloud Storage

Key Vocabulary	
Server	A computer that delivers data between machines that are connected to a local network.
Downloading	A file or document can be used when you are not connected to the internet.
Uploading	A file or documents can be used by you or other with access when connected to the internet.
Synchronising	Is when files held on two devices are updated to make sure that both have the same content.

What is cloud storage?

Files and folders are stored remotely rather than on a PC or device.

The files are stored on **servers** so they can be accessed via the internet.
When you want to access the media, the data is **downloaded** or streamed to the device you wish to use it on.
It remains in the file in the cloud unless you delete it.
Data on your device can also be **uploaded** to the cloud.

When is cloud storage available?

- Only when there's an internet connection.
- If the connection is broken access will be terminated.
- The speed of the connection will impact file upload speed and download stream speed.
- If there is a suitable connection, data and files in the cloud can be accessed 24/7

Features and usage of cloud storage:

- ISPs often give users a cloud storage allocation as part of a phone or tablet contract
- **Scalability** – you can pay for extra storage.
- Services can also be provided by third parties
- Cloud storage is useful for storing backups of your files. Copies of the files are made on different servers so that they are protected if attacked or in case of a natural disaster such as fire or flood
- You can **synchronise** with the cloud.

What can be stored in the cloud?

- Images/Videos
- Emails
- Contact info
- App Back Ups

What do you store on the cloud?

Cloud Storage Providers:

Benefits of cloud storage	Drawbacks of cloud storage
You can access your data from any device that has an internet connection and a web browser.	If there is no connection you can not access your data. Slow connection also will hinder your experience.
Scalable – You can purchase more storage space easily.	Some providers offer limited storagespace for free, but additional space can be expensive
The data and its security is managedby the provider.	You have no control where or how your data is stored. You must trust the provider to keep your data confidential.

There are two main ways of accessing online applications.

1.Web-based applications which run entirely through browsers
2.Cloud-based applications where your local services and cloud service work together to provide a service.

Benefits of online applications	Drawbacks of online applications
No installation	Must have a reliable internet connection.
Cost effective	
No need for updates	
Accessible from anywhere	
Direct access	

What is file sharing?

Two or more people can work on the same document at the same time.

Benefits of collaboration tools

Collaboration tools allow users to:

- Add comments to documents
- Track changes made to the document
- Use services such as live editing
- Use chat facilities to discuss proposed changes to documents, plans or drawings before these changes are made in the file.

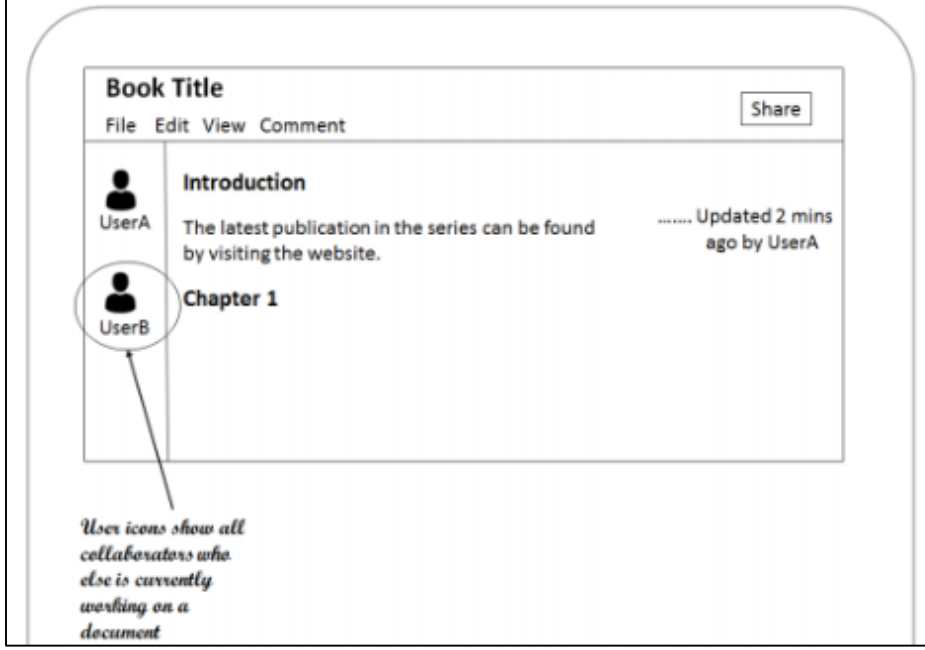
Example exam question

PublishShare works with writers from all over the world. They use cloud computing technologies for employees and writers to collaborate.

(c) Annotate the diagram to explain how **two** different features of this cloud computing system can be used to aid collaboration.

Your annotation should include the identification of each feature and an explanation to show how the feature can be used to aid collaboration. An example has been provided

(4)



Key Vocabulary	
Stakeholders	These are people with a financial interest or investment In a business or organisation
Downtime	A period of time when a computer and it's services are unavailable.
Geo-data	Geographical information stored in a way it can be used by your device. i.e. your location.

The most common platform types:

- Desktop client
- Notebook
- Tablet
- Smartphone

Features that affect platform selection:

- Screen size
- Portability
- Processing power
- RAM
- Storage capacity
- User interface (keyboard, mouse, touchscreen, voice control, etc)
- Operating system (Apple iOS, Microsoft Windows, Android etc)

What might an organisation consider when selecting a cloud platform?

- Security methods
- Amount of storage space
- Ease of use
- Frequency of updates
- Accessibility
- Cost
- Interface design

Example exam question

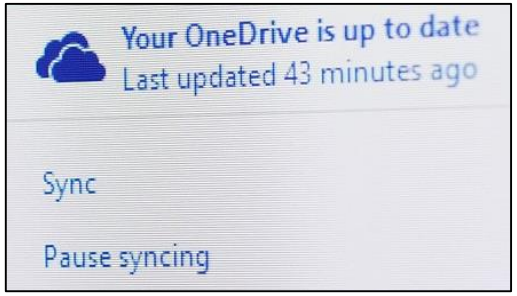
A photographer/ journalist at a football match takes hundreds of pictures during a game. They will need to select the best picture and write a story before the deadline 2 hours after the game has finished. Using the features below which device would be most suited for his job? [4]

- Screen Size
- Portability (how easy it is to move around)
- Storage capacity
- User interface

Key Vocabulary	
Synchronisation	Process of making two or more data storage devices or programs (in the same or different computers) having exactly the same information at a given time.

Notifications

Cloud systems will send you notifications based on your activity, or what team members with shared access to the same folders you are working on.



Synchronising content over devices

Sometimes applications and files are located on an organisation's own system or user's PC, but they could be in the cloud.

Most organisations and many individuals use a combination of both.

When using a combination of both, synchronisation is particularly important to make sure that all versions of the files are exactly the same.
e.g. A sales person has files stored on their work PC, which are then synchronised to their laptop and are available via a smartphone.

Syncing Apple devices using iTunes:

A user can choose to automatically back up their device to the cloud, and to only sync ticked songs and videos (rather than all content) over Wi-Fi.
If the user has several devices that access the same cloud content, all the devices would be updated.

Online/Offline Working

Many workers are not necessarily in the office every day, they may work in another geographically remote office, at home, or while travelling.
When working offline, files can be saved in a shared area.
They will not be saved immediately in the cloud, but copies of the files are also saved offline on the user's device. When internet access become available, the files will be automatically synced.

Connecting to the internet:

Most laptops connect to the internet using Wi-Fi.
If no Wi-Fi connection is available, it may be possible to **tether** laptops to smartphones.

In this way the phone is being used as a **personal hotspot**, which allows the laptop to connect to the internet via the phone.

If no internet connection is possible, the user will work offline and upload or synchronise the content with the relevant systems when an internet connection is available.

Example exam question

1. Explain why you should sync content between devices and systems.

2. Explain how a personal hotspot helps with synchronisation.

There are different factors that organisations will have to consider when choosing cloud technologies that will work for them and their situation. Some of these include:

- The Disaster recovery policies
- Data Security
- Compatibility issues

Disaster Recovery Policies

Most cloud technology services offer backup services as part of their set-up costs.

Automatic backing up is usually carried out at quiet periods.

A disaster recovery policy is typically designed to set out the **actions** that will need to take place after a disaster, **for example** an **attack or natural disaster**, such as a fire or flood, **to restore** an organisation's **services and processes** as quickly as possible.

Cloud technologies can generally be relied on to:

- Be unaffected by attack of disaster as they are located away from the organisation.
- Have appropriate nightly backups - in the event of a disaster very little data is lost.
- Be protected by good security.

Data security

Most cloud computing companies will have several strategies in place to protect the security of their customer information.
Any breach could damage their public image and lead to serious consequences for the organisation such as loss of customers and legal action.

As a result, the cloud technologies service provider will employ a range of security measures, including keeping their digital systems protected at their large data centres, where many computers are located under one roof.
They will also control access to data and are storing data safely and in an encrypted format where necessary.
Broken or outdated digital systems will be appropriately disposed of.

Compatibility

Compatibility isn't usually an issue for organisations when choosing cloud technologies.
Most cloud technologies use well-supported and documented operating systems such as Microsoft Windows or Linux.
This should enable organisations to run any combination of popular applications and services without an issue.

Benefits of disaster recovery policies	Drawbacks of disaster recovery policies
The can reduce the amount of time it takes to recover following a cyber security disaster.	It is not always possible to think of every single risk that could occur before an attack iscarried out.
The set out the roles of each person so everybody knows what to do following an attack.	Once the policy has been created, it needs to be continually updated to ensure new threats have been accounted for.

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A1 Modern Technologies – Maintenance, Set-up and Performance

Key Vocabulary	
Virtual Machines	Software applications that are designed to behave as if they are a whole computer.
System administrator	A person who is responsible for a technology to make sure they are maintained and reliable.
Spam	Electronic junk mail, usually sent with a commercial purpose.

Maintenance of cloud computing solutions

Usually automatic because solution providers regularly update processes, which keep the **virtual machines (VMs)** up to date and make sure that the solutions stay healthy and secure.

Organisations may add their own services and updates as part of their security policies.

Most cloud computing solutions have web-based dashboards that can monitor activity levels, such as CPU usage, disk space and network communication.

Additional settings can email the organisation's **system administrator** about potential problems, including high CPU usage, low available disk space etc.

Benefits of cloud technologies	Drawbacks of cloud technologies
Technologies are generally secure 'out of the box'	So services may not be allowed. E.g. mail servers.
They are up to date	A good internet connection is required.
Automatic backups may be created as part of the plan.	Organisational data is stored on the internet.
Solutions can be depilated easily	Pricing plans maybe more expensive than expected.
Solutions can be re provisioned quickly and without fuss.	Incompatible product may cause issues with data transfer.
Technologies may require less monitoring.	
Technologies may require less manual intervention.	
Disruption of service is generally rare.	

Downtime

Downtime is usually limited on a cloud computing solution.

Downtime of just a few minutes can be a serious issue for organisations that rely on a continuous 24-hour service.

Downtime can be caused by:

- Interrupted internet connectivity,
- Cyberattacks,
- Updates

Performance considerations

- A fast broadband connection is required or the responsiveness to user requests and synchronisation of devices may be slow.
- Service or storage needs to satisfy all the requirements of the organisation.
- May need to be scalable.
- Software must be responsive to users.
- Proposed cloud software will run on any devices that are used by employees.

Set up Considerations

Setting up a server requires	Setting up a cloud computing VM solutions requires.
•Hardware purchase •Hardware build or customisation. •Operating system installation and configuration •Applications and services installation and configuration •Protecting from external threats. •Test network connectivity.	•Selecting the cloud computing solution provider. •Creating an account and payment info. •Select type of cloud computing solution required. •Selecting operating system and role of solution •Deploying the device •Performing additional configuration as required.

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – Collaborative Technologies

Key Vocabulary	
Version Control	Records changes to documents and files over time so that all versions can be recalled if needed.

Collaborative Technologies

Collaborative technologies enable staff to work together more effectively, allowing them to communicate and share information and documentation more easily.

There are lots of technologies and software to help employees to communicate and collaborate.

e.g. employees on different locations could work together on the designs for a new product, working in the same files at the same time.

Benefit of collaborative technologies	Description
Global and multicultural workplace	Can help build relationships between people of different ages, gender, religion or culture. Leads to increased creativity and diversity in the workplace.
Inclusivity	Technology has provided functionality to help those who have limitations or disabilities. e.g. people with visual impairments can work on the same documents as people with no impairment by using software to enlarge the text.
24/7/365	Services or facilities open 24/7/365 e.g. Internet content is available 24/7/365 – users are able to access pages at any time of the day or night.
Team flexibility	Teams who work in different locations, countries or time zones can use technologies that allow them to share information and to contribute to projects from remote locations and at different times of the day. The working day can be lengthened e.g. one team can finish as another team in a different time zone begins.

Type of collaborative technology	Examples	Uses
Interoffice chat programmes	LiveChat, Office Chat	Useful for answering business questions more quickly than through email
Conferencing software	GoToMeeting	Used to support meetings without employees having to travel
Project support technologies	Google Drive,DropBox	Support document sharing
Project support technologies	FlockDraw	Enables team members to edit images simultaneously in real time

Version Control

If several people are working on the same document, they could each save their document onto their computer, which would create several versions of the same document.
They could also overwrite each other's work.

One way to overcome this is to use **version control** which can have the following features:
Workflow – only one person can work on a document at a time.
One person at a time has edit access, the other people only have read access.
History – a of what has been changed and who has changed it is kept.
You can see the changes that have been made and then agree or disagree with them.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – Managing teams: Communication and Collaboration

Tools for collaboration

Modern technologies have made it much easier for managers to monitor the activities of their teams.

There are many tools that can be used to promote collaboration e.g. BaseCamp.
These tools include several features, such as:

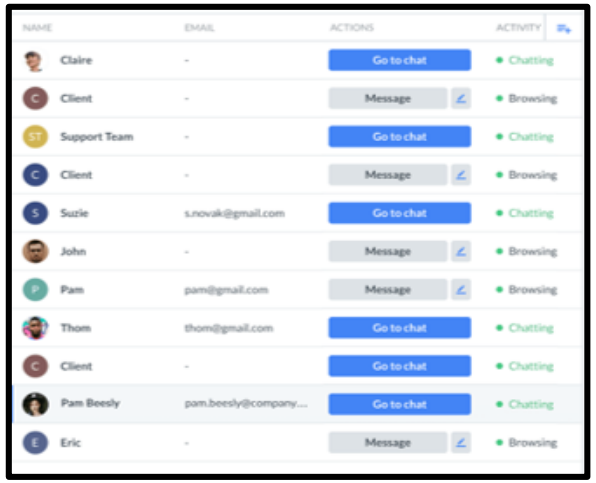
- To-do area,
- Message board,
- Schedule.

Communicating as a team

Many organisations used chat programs to help staff in different departments or locations have a quick discussion.

One of the main benefits of this software is that you can see which of your colleagues is online, so it is clear who can be contacted.

Other available settings include "busy", "unavailable" or "offline".



Benefits of using collaborative and communication software to manage teams:

- Storing and managing relevant working files in a single location.
- Ensuring that the file being worked on is the most up to date (as there is only one working copy of the file).
- Archiving previous versions of the file.
- Using features of the software to allow team members to work on files at the same time.
- Communicating with the whole team simultaneously.
- Providing group support by the manager.
- Saving discussions (in case they are needed later).

Example Exam Question

The use of collaborative technologies will allow PublishShare's employees to work from home.

(d) Explain **two** benefits to PublishShare of allowing its employees to work from home.

(4)

1 .....

.....

.....

2 .....

.....

.....

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – Managing Teams: Scheduling and Planning

Key Vocabulary	
URL	stands for **U**niform **R**esource **L**ocator and is the address of a page on the World Wide Web.

Scheduling and Planning

When you create a new project in planning software you can set a start and end date and it will automatically calculate the number of days involved.

When managing teams, you could use project planning software to allocate tasks and control the schedule.

Setting up a team

- You can set up a team by inviting team members using their email address.
- The team member is then notified and is given a URL and password to access the system.
- When you invite users you can assign a role to them which will determine their level of access to the system.
- To add activities to the project you use the calendar function.
- Each participant then receives an email notifying them of any additions or changes to the calendar.

Benefits of using scheduling and planning software to manage and work within teams	
Benefit	**Description**
Access	Files and folders can be stored in one place so that all members of the team canaccess them.
Tracking	Project managers can track progress and monitor the activities of teammembers.
Version control/archive	Older versions of documents can be archived to ensure the documents being used are always the most recent ones. The archive is a file of all the previousversions of documents.
Timelines and deadlines	Project deadlines and key milestones can be automatically synchronised with team member calendars.
Communication andcollaboration	Software automatically allows for variations in time zones. This enables workers in different time zones to see when they need to do tasks in their own time zone

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – Communication with Stakeholders

Communication Platforms

There are lots of communication platforms available, for example:

- Email,
- Social media,
- Text messages

Communication with Stakeholders

Organisations use a wide selection of communication technologies to connect with their stakeholders, from their corporate websites to social media platforms such as Facebook.

What is a stakeholder?

An organisation's stakeholders include:

- Customers,
- Employees,
- Suppliers,
- Anyone else with an interest in the organisation.

Technologies for Communication

Channels	Description
Websites	Provide a range of content, including information on products or services, prices, stock information and special offers so that customers can buy items online.
Social media	Organisations can communicate in a much more relaxed way e.g. customers can ask for advice about a product.
Email	More formal method of communication that has largely taken over from letters as the email is received almost instantly.
Voice communication	Brings people together without them being in the same place. Can be live video as wellas audio. This technology is often used to deliver training. The presenter can display presentationslides on the screen and participants can hear the presenter speak.
Live chat	Some organisations offer technical support and customer service using live chat, where a text messaging app is used to support a conversation. Users usually have to log into their account to access this feature.

How to choose the right communication technologies

Organisations must think carefully about which communication channels they should use in different situations to share information, data or other media. Communications can largely be classified as either private/direct or public.

Private Communications	Public Communications
Communications between specific individuals. Only the people involved should be able to see the messages. For example: Customer queries, such as order/payment information or requests for payment Customer payment details, including account details and payment methods Customer contact details, such as phone numbers or changes of address	Anyone can see the information that has been communicated. For example: Product information, such as special features, Price reductions and other special offers, Advice on using a product.

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – Accessibility and Inclusivity

Key Vocabulary	
ALT Text	is alternative text that describes an onscreen image for users with visual impairments.

Accessibility and Inclusivity

Computers should be capable of being accessed and used by everyone, but some users have physical challenges that make aspects of computer use difficult or impossible.

Technologies that help users overcome some of these challenges are becoming increasingly available.

Interface Design

Organisations must think about how a website looks when it is viewed on different devices.
The screen size affects what is visible and how it is displayed.
Websites that do not adjust for different devices are known as **non-responsive** websites.

For example, the Amazon website.
Amazon's solution is to provide apps for different devices to make sure their content looks its best on any device.
They also have a mobile website that reflects the app design.

Interface Layout

The layout of screens also contributes to inclusivity and accessibility of web content.

The content should be simply laid out with clear differences between the sections, with simple input and navigation controls that allow all users to easily interact with what is onscreen.

The screen size affects what can be displayed and how it is displayed.

Accessibility Features

Most operating systems have built-in accessibility features, such as magnifiers, the option to change the colour schemes and even to use the computer without a display, mouse or keyboard.

Other accessibility tools available include:

- Screen readers – which read the content of the screen to the user.
- Software that converts speech to text
- ALT text – allows the addition of text-based description of each image on a website for the benefit of blind or partially sighted users.

Inclusivity

Inclusivity is about the different ways to involve employees who have useful skills to contribute, but who are not able to work in the traditional way
e.g. someone recovering from an operation who is not able to drive to work yet but could work from home.

Organisations can allow their employees to work more flexibly permanently.

This could be by allowing them to work hours that suit their childcare commitments or to choose working hours and locations that suit them.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – How Modern Technologies Impact on an Organisation (Part 1)

Key Vocabulary	
Distributed Data	Split into lots of bits and stored in different places.
Dispersed Data	Multiple copies of the same data in different locations.

Impacts of infrastructure on an organisation:

- Costing what is needed to buy and set up services
- Training for staff
- Implementing and testing time for the technology before staff use it in their work
- Maintaining technology – if software is not updated it may not work correctly
- Running costs of hardware e.g. printer ink
- Implementing a strategy to ensure that data is backed up and secure

Managers must weigh up the costs of technology against the benefits it will bring.

Security of distributed/dispersed data

Data that is **distributed** or **dispersed** can be stored over more than one server and network.
The locations of the different bits or copies of data need to be mapped so that the data can be found when it is needed.

Benefits and Drawbacks of Technologies

Technologies	Description	Benefits	Drawbacks
Communication technologies (devices)	It is now common practice for managers to be issued with laptops, mobile phones and tablets	Less paperwork to carry as files can be accessed electronically	Can be intrusive as staff can be contacted day and night, which can impact on the employee's work/life balance
Local platforms	Software installed andused locally	May run faster than a web-based alternative	Cannot be accessed outside the office
Web-based platforms	Software installed andused online	Can be accessed fromanywhere	May run more slowly than local alternatives connectivity is poor or demand is high
Availability	Because of the costs of technology, many organisations try and find different ways of using what they have, rather than simply buying more.		

Benefits of distributed data	Drawbacks of distributed data
The data is less likely to be lost because it is not all in one place.	There are more locations to keep secure
Security is greater because criminals would not know where the data is being stored.	Locations of data need to be tracked so that thesystem knows where the data is
The data can be accessed over different networks	It can take a little longer to access data that is further away
Greater reliability	Additional software is often required

Organisations that use technology are usually accessible 24/7

Benefits and drawbacks for customers of 24/7 access	
Benefits	**Drawbacks**
Orders can be placed and accounts accessed at any time of the day or night	Usually you must wait until your purchase is delivered and pay extra if you want it delivered quickly
No need to stand at the till to pay for purchases as you canbuy online	You cannot see or touch the product before you buy it
Lower prices as there is more competition	Security worries – it is a legitimate website?
More choice as you can access a much wider range ofproducts	You often must pay for delivery, or higher rates for fasterdelivery
No need to spend money on transport or parking	Returning items can be challenging and you may have to waitto receive a refund.
Able to check your bank balance and pay bills at any time ofthe day or night	
Ability to transfer money from one account to anotherwithout having to go to the bank	

Benefits and drawbacks for organisations of 24/7 access	
Benefits	**Drawbacks**
You can access more customers over a widergeographical area. Your potential customer base isanyone, anywhere in the world, you are only limited onwhere you are willing and able to ship products.	Many customers still like to visit a shop or business and speak to a person
You may not have to pay the costs of having premises.Many online businesses do not have a presence in the high street.	You have to make sure you build good relationshipswith customers as you will have more competition.
Online businesses may be cheaper to set up.	
You can collect information about your customer'sbrowsing and shopping habits, which could enable youto improve how you target different types of customerswith your different products	

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – How Technologies Impact the way Organisation Operate

Key Vocabulary	
Wiki	this is a web page (or pages) that has been developed collaboratively by a group of people

Digital technologies have made communication and working together in organisations much more efficient and accessible.

Benefits and Drawbacks of Collaborative Technologies.		
Technology	**Benefits**	**Drawbacks**
File sharing	Using software such as OneDrive or DropBox enables employees to work together and share development responsibilities and activities	There is a new to make sure that employees are always using the most up-to-date version of a document
Wikis	Web pages that can easily be edited by members of a team e.g. Wikipedia	You need to check that information is correct, particularly if you are responsible for a commercial wiki
Blogs	This is an abbreviation of web logs, which are often created about a specific topic	They need to be regularly updated to keep their audience interested
Chat Systems	Interoffice chat systems are useful for helping staff access information or those seeking decisions quickly	These systems can be time wasting if theyarea used for social rather than business discussions
Tele/videoconferencing	Staff in different locations can attend meetings virtually which saves significant travel time and money and enables collaboration and decision-making	A high bandwidth communication link is required to transmit and receive high-quality images.

Technology and Accessibility

Many organisations now support the use of wearable technologies.
The benefit for staff is that they are easily accessible, they can receive phone calls and read emails without accessing their phones.

Many of these wearable technologies have sensors that can capture health and fitness information, so staff are reluctant to wear them as the organisation has access to data that they want to keep private.
By law, organisations are required to make accessibility adaptations to the working environment if a member of staff has an accessibility or health-related issue.

Technology and Remote Working

More and more people can access paid work that does not require them to go to a specific place of work.
The benefits to the organisation are:

- Access to a wider and more diverse range of potential employees.
- Less office space is required if some staff work from home, resulting in cost savings.

Drawbacks to the organisation:

- Employee is not on site, limiting the interaction between colleagues and opportunities for ad hoc meetings and impromptu discussions.

Some employees choose to install monitoring software on their employee's computers to check the hours they are working and the activities they complete. This can be demoralising to employees who do not feel trusted.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim A – A2 Impact of Modern Technologies – How Technologies Impact on Individuals

How technology impacts individuals

Devices like smartphones have changed the way we communicate and entertain ourselves.
For example: We can play music, videos or games on handheld devices when travelling. We can stream music while working.

Using technology has now become common in the workplace and has made many aspects of work much easier, such as being able to access a work diary from anywhere.

Impact on individual wellbeing

Technology impacts on the way you feel about yourself and the world around you.

Technology can impact positively on the wellbeing of individuals, but this is not always the case ,for some people there can be negative consequences as well.

Working flexibly and choosing your working style

If you can work flexibly, during hours that suit you and your family, this can improve your morale and reduce personal stress levels.

Working flexibly does require employees to be self-disciplined and organisations may monitor your activity.

Impact of Technology

The impact of technology	What it really means	Benefit or drawback
Contact with others	Can talk to other people about thing in your life that are going well or badly, but too muchcontact can be intrusive	Benefit and drawback
Self-confidence	Being able to research things makes your more confident, if you are sure the information is correct and reliable	Benefit
Lack of confidence	Some of us need reassurance about what we are doing and we need input from others to feel confident about what we are doing	Drawback
Separation from a stressful environment	Technology means that you can escape into computer games, videos or music to remove yourself from stress	Benefit
Control of your ownschedule	People who use electronic diaries or schedules often feel more in control of their personal and working lives because they know where they need to be	Benefit
Ability to control your schedule to meet the needs of your family	Technology gives you the confidence that you can adapt your schedule to meet the needs of your family	Benefit
Less time commuting to or between offices	Technology could make you more productive if you can work from home or can be based in a single place and take part in virtual meetings	Benefit
Loneliness	Just because you can talk to someone via a device or app does not mean that you are not lonely	Drawback
Depression	People who work lots on their own can become isolated and depressed because they are notinteracting with others	Drawback

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B1 – Threats to data: Why Systems are attacked

Key Vocabulary	
Intellectual Property	An idea that you invented that belongs to you, for example, an image that is copyrighted.
Ransomware	A form of **malware**, usually infecting unprotected digital systems, occurring when users open malicious email attachments.
Malware	A malicious form of software that is transferred to, and then executed on, a user's machine to damage or disrupt the system or allow unauthorised access to data.
Denial-of-Service (DoS) attacks	Attack a remote computer by making it unable to respond to legitimate user requests.
Cybersecurity	The combination of policies, procedures, technologies and the actions of individuals to protect from both internal and external threats.

Organisations have become reliant on digital systems to hold data and perform vital business functions.
Many organisations have their digital systems attacked daily.
The reasons these attacks may occur are varied

Data and information theft

Data and information both have value as they can be sold for financial gain.
This can be done by stealing customer payment information and then using it to purchase goods illegally.
Breaches of data and information are a major cause of identity theft.

Fun/ Challenge

- Hackers may attack systems for the thrill, adrenaline rush or a sense of personal achievement.
- They may view increased security as a technical challenge and enjoy trying to get past it.
- They may also get recognition from their peers when they successfully hack into systems.

Disruption

Any attack that prevents an organisation from operating normally causes operational chaos, loss of earnings and reputational damage.
Disruption can be caused in many ways e.g. defacing a website or **Denial-of-service (DoS) attacks**

Motivations may be: financial/social/political reasons.

Industrial Espionage

Intellectual property (designs, business strategy etc) can be stolen through organised cyberattacks.

These types of assets can be highly valuable, leading to cheaper, fake copies of products being sold and the original organisation suffering a loss of income.

Financial Gain

A very simple motive: money.

Extorting money from victims of a cyberattack is common practice.

Personal Attack

The most common type of personal attack is made by ex-employees holding a grudge against their former employer, perhaps feeling they have been unfairly treated or suffered a form of emotional distress.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B1 – Threats to data: External Threats to Digital Systems and Data Security

Key Vocabulary	
Social Engineering	The act of getting users to share sensitive information through a false pretext (commonly known as 'blagging')
Phishing	A cyberattack that sends spam messages to try and trick people to reply with desired information.
Pharming	A cyberattack that uses malware to direct a user to a fake website that requests information.

External attack methods include:

- Unauthorised access/hacking
- Phishing
- Pharming
- Man-in-the-middle attacks

Unauthorised access/Hacking:

'Black-hat' hacking - users attempt to gain access to remote systems without permission from the owners to do so legally

'White hat' or ethical hacking - Hacking legally performed by paid specialists who are testing the security systems for a company is called

'Grey hat' hacking - hackers test security without permission, but don't exploit any vulnerabilities for personal gain.

Pharming

A type of cyber attack

User is directed to a fake website thinking it is real and they then enter confidential details such as usernames and passwords.

The cybercriminal uses these captured details to log into the real website and commit illegal acts e.g. withdrawing money, purchasing goods, downloading personal files or sending fraudulent emails

Man in the Middle Attacks

A form of cyberattack where the communication between 2 devices, such as a user and a web server, is intercepted and potentially tampered with.

Encryption can protect against this form of hacking as any intercepted data cannot be easily used.
Cybersecurity specialists also suggest that users would be safer if they did not use Wi-Fi.

Phishing

A form of social engineering and a very common form of cyberattack.
Spoof emails are sent that pretend to be from a genuine company.
The user is fooled into thinking its from a legitimate source.
Usernames, passwords and credit card numbers are the most commonly captured personal information.
These can then be sold for profit to other criminals or users to illegally purchase goods or services.

Spear phishing is an attack targeting specific organisations or individuals.

v

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B1 – Threats to data: Internal Threats to Digital Systems and Data Security

Key Vocabulary	
Productivity	a measure of effectiveness – how long it takes an employee to produce an item for sale.

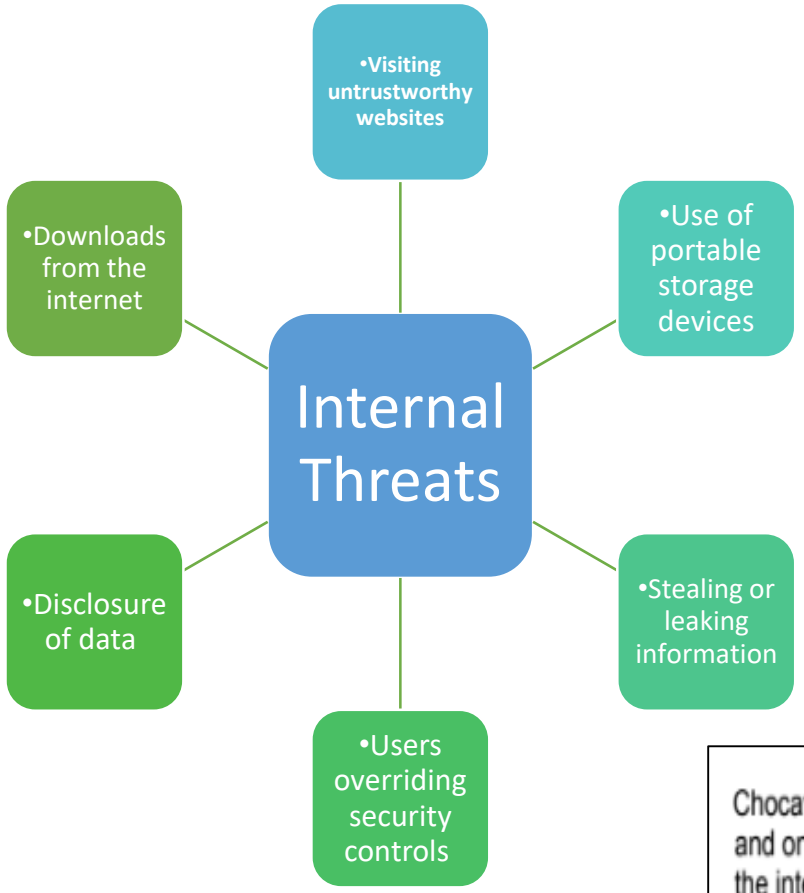
Internal Threats

Some internal threats happen because of accidents, mistakes or poor choices made by an organisation's employees. However, a disgruntled employee could do something malicious.

For example:

- Delete customer records
- Steal confidential information
- Create fake invoices that will be paid to their own bank account
- Install malware

Protecting an organisation against internal threats is as important as protecting against external ones.



Impacts of security breach	
Immediate Impacts	**Longer-term Impacts**
•Data loss •Lost sales •Downtime •Reduction in productivity	Damage to the organisation's public image which could lead to: •Financial loss •Potential legal action

Example Exam Question

Chocawoca's recipes are kept on secure servers in their secret recipe rooms and only certain staff have access to these recipes. They are concerned about the internal threats to this vital data.

(b) Explain **two** possible internal threats to Chocawoca's recipes.

(4)

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B2 – Prevention and Management of Threats to Data: User Access Restriction

Physical Security

Benefits	Drawbacks
Act as a deterrent and deter attackers.	Often more expensive to purchase
Stop attackers from gaining direct and physical access to locations where data is stored.	Building work may be required.
Automatically and secretly call the police if an attacker is detected,	Some methods of physical security, such as CCTV, do not stop data from being stolen

Example Security techniques:

- Electronic Swipe Lock
- Secure Device
- CCTV Camera

Biometrics

Requires individuals to use part of their body to prove their identity.

- Common biometric examples include:
- Eye (retina or iris pattern) scan
- Fingerprint identification
- Hand geometry (shape of user's hand)
- Voice analysis
- Facial recognition
- Gait analysis (how a user walks)
- Handwriting analysis

Benefits	Drawbacks
•Users don't need to remember lots of different passwords or keep updating them. •More secure as they cannot be guessed, lost or forgotten. •Can take less management because users are less likely to be 'locked out' or need to have their user accounts reset.	•More expensive as you need specialist hardware devices to set them up. •They can easily spread germs, e.g. if lots of users are using the finger print scanner then germs can be easily spread. •Some users may feel that it is an invasion of their privacy by having their biometric data stored.

Passwords

The use of passwords is a traditional security measure to control access to digital systems.

There are other forms of passwords:

- Patterns that can be drawn connecting a series of dots
- Gesture passwords - can be used with touchscreen devices where the user draws a shape.

Benefits	Drawbacks
•They are simple and easy to use. •There are no costs involved as they require no specialist hardware to setup.	•They are only effective if users keep their passwords secret. •A strong password can be hard to remember. •Specialist software can be used by attackers to try and guess the user's passwords. •Users can find it hard to remember lots of different passwords.

Two-factor Authentication

A popular form of multifactor authentication and is used when just a password or PIN is not considered sufficient.
It works by asking the user to supply two forms of identification.

Benefits	Drawbacks
•It is more secure. •No extra equipment is needed as users can use items they already have to authenticate themselves, e.g. their mobile phones.	•It is possible that some factors may get lost e.g. you may lose your swipe card. •The recovery options that are used to reset your account are easy to get through, which could be exploited by attackers. •It can take longer to gain access

CHURCH STRETTON SCHOOL	BTEC DIT Component 3 Knowledge Organiser	Learning Aim B Cyber Security – B2 – Prevention and Management of Threats to Data: Data Level Protection: firewalls and anti-virus software (1)

Key Vocabulary	
Firewall	A device that protects an IT system (or network) from unauthorised access by blocking 'bad' network traffic.
Local Area Network (LAN)	A network based on geographical location, such as an office or a school
Access Control List (ACL)	A list that tells the network which data can be sent and received.
Shoulder Surfing	Obtaining sensitive personal information from a user by literally looking over their shoulder while they use digital devices e.g. computers or cash machines.
Session Cookies	Data stored by the web browser until it is closed
Worms	Small computer programs that can spread to other programs.
Trojans	Types of malware disguised as legitimate programs.
Rootkit	Collection of tools or programs that allow an unauthorised user to obtain undetected control of a computer system.
Spyware	Software that is installed on a device without the user's knowledge. It can gather information about their computer activities by transmitting data secretly from their hard drive.

Firewalls

- Form the first line of defence in protecting digital systems from external threats such as cyberattacks and viruses.
- Can be hardware or software based
- Work by using a set of rules that filter and reject unwanted or suspicious network packets arriving from a remote network.

Hardware firewall	Software Firewall
Sit between an external network and an internal connection e.g. the internet and a local area network (LAN)	A digital system can host its own firewall service, which blocks network data travelling in and out. Applications can also be stopped from sending and/or receiving certain packets of network data. They do this by creating a set of rules that determine which packets of data are sent and received – an access control list (ACL).

Benefits of firewalls	Drawbacks of firewalls
They can stop attackers from gaining unauthorised access to a device.	Firewalls can block legitimate things.
You can customise the firewall settings to meet the needs of your organisation.	Can make the performance of a computer or network a lot slower.
Software firewalls are easy to install.	Highly effective firewalls can be very expensive.

Modern software design aims to make applications easier to use, often including various tricks that can assist user inputs.
Some techniques can improve security; others can cause issues.

Common techniques used to make applications easier to use

Obscuring data entry	Common technique to solve **shoulder surfing** when using secure logins in a public place is to obscure the entry of sensitive data e.g. passwords.
Autocomplete	Autocomplete is a technique where an application will recognise a familiar input and make suggestions from previous inputs. If used on a publicly accessed IT system it can be a security risk.
"Stay logged in"	Web applications often use **session cookies** to keep a user logged in, even if they leave a page and later return to it. Can be a security risk if a different user gains access to the IT system before the web browser is closed and the session cookie is cleared.

Anti-Virus Software

Anti-virus software monitors a digital system, attempting to identify and remove malicious software before it can cause damage.
Most viruses infect a digital system when the unsuspecting user opens infected email attachments.
Worm viruses can replicate themselves from device to device via the network.

Different types of viruses include:
- Ransomware
- Worms
- Trojans
- Rootkit
- Spyware

Benefits of anti-virus software	Drawbacks of anti-virus software
Can stop files that contain viruses from accessing your computer system.	Needs to be continually updated to ensure it can detect new viruses.
Some anti-virus software is free to download.	Can make the performance of a computer or network slow.
If a virus is not yet known, anti-virus software is able to monitor the behaviour of files to see if they are showing any virus characteristics	Highly effective anti-virus software can be very expensive.

Example Exam Question

At present, staff who work at Chocawoca use a card entry system to gain access to their secret recipe rooms, cards are swiped at the entrance. They are considering changing this to use a biometric system as they think this will improve security.

(c) Explain **two** benefits of biometric systems to Chocawoca.

(4)

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B2 – Prevention and Management of Threats to Data: Data Level Protection: Device Hardening and Encryption

Key Vocabulary	
Vulnerable	Describes a flaw of weakness in the design, implementation or configuration of a system. Known vulnerabilities can be exploited by 'black hats' to attack a digital system.
Security patches	Additional settings or program codes that fix vulnerabilities in applications, operating systems and device firmware, and are usually downloaded from the manufacturer.
Privilege	A set of rules that allows users to use specific components or access data folder or files.

Device Hardening

Digital systems may have default settings or weaknesses that can make them (and their data) **vulnerable** to attack.
The process known as 'device hardening' attempts to resolve these issues.
Device hardening techniques:

- Installing a firewall
- Installing anti-virus (and anti-spyware) software
- Applying **security patches** and updates
- Using encryption
- Closing unused network ports
- Removing non-essential programs or services
- Restricting user access (called the principle of 'least **privilege**')

Encryption

It is common practice to encrypt data when it is stored and when it is being transmitted between IT systems.
Stored data is a popular target for cyberattacks and unencrypted (plaintext) data is considered insecure and a security risk. - One solution is to encrypt this stored data.

Vast quantities of personal data are transmitted from web browsers to web severs and back again, especially in web applications e.g. social networking and online banking.

Organisation web servers can use a digital signature that can be transmitted to a web browser to prove its identity and encrypt data transmissions between them.

You can tell if a connection [illegible] e HTTPS prefix on a website address.

Benefits	Drawbacks
•Scrambles data so that others cannot easily read it. •Ensures that organisations comply with data protection laws.	•Does not stop data from being stolen. •Encrypting a large amount of data can take time. •Encryption methods need to continually 'evolve' and change as attackers find new ways to access data.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B2 – Prevention and Management of Threats to Data: Data Level Protection: Finding Weaknesses and System Improvements

Organisations have responsibility to secure their IT systems to protect the personal and sensitive data they store and process.
Assessing the security of IT systems objectively can be difficult to do, so sometimes external help is required

Ethical Hacking

A process where an individual or a team of penetration testers are asked by an organisation to simulate an attack on its IT system to highlight any weakness and vulnerability.

To start with, the hackers are given little information about the system and will identify weaknesses and then exploit them to see if sensitive data or services can be accessed.

White hat hacker – an IT specialist who is invited to discover vulnerabilities in a system and report them to the organisation or author.

Grey hat hacker – an IT specialist who discovers vulnerabilities in a system, typically without invitation, but does not exploit them for personal gain (although they might make the information publicly known).

Benefits	Drawbacks
Can see if the security of your network is able to withstand the skills of expert attackers.	Can be very expensive to hire professionals with the necessary skills.
Can help to find 'loopholes' in your network security in order to make it better.	Depends on the trustworthiness of the ethical hacker. Some may abuse their position.
The security of a system can keep evolving when loopholes in the network security have been found.	Some people may view ethical hacking as an invasion of privacy if others are able to view their data.

Penetration Testing

Aka 'pen' testing.
A systematic process used by ethical hackers to determine how secure an IT system is.

Frequent vulnerabilities that ethical hackers uncover when attacking a system:

- Unpatched operating systems and applications.
- Web applications that have not been well programmed, leaving them insecure.
- Data that has not been encrypted.
- Poor security practices

Stages of penetration testing:

1. Authorisation to penetration test
2. Discover vulnerabilities and weaknesses
3. Exploit weaknesses (without disruption)
4. Document weaknesses
5. Recommend security improvements

Penetration Testing Report

The findings of penetration testing are presented to the organisation as a formal report, including recommendations that may resolve the issues found.

The report is used to harden the security, addressing the issues found.

The process may then be repeated until the organisation is sufficiently confident in its systems

Security Policies

To make sure that all employees in all locations follow the same code of conduct organisations create policies that set out the responsibilities of staff.

These policies detail how staff are expected to behave and what procedures they should follow in the event of a disaster.

Most security policies are implemented by IT and technical staff..

Examples of security policies include:

- System security
- Data security
- Compliance (with regulations and legislation)
- Environmental (including disposal of old equipment and waste products)
- Disaster recovery
- Data recovery
- Infrastructure (updating and replacing hardware and software)
- Responsible use policies (including email and internet use policies)

Planning for disaster recovery

Policies exist to increase the robustness of IT systems and data and to plan for what should happen in the event of a disaster.

Disasters can come in many forms:

- Theft of data (having systems hacked or laptops/devices stolen)
- Virus or other malware infection
- Data loss (accidental deletion or intentional sabotage)
- Fire or flood
- Mechanical failure of equipment

To ensure the organisation can become operational again as quickly as possible, a detailed plan is created.

Disaster Recovery Plan

Consideration	Description
Identifying potential risks	Identify potential risks to the system and how each risk will affect the computer system and data
Who is responsible for which actions in the event of a disaster	Staff are given specific recovery tasks to avoid anything being duplicated or forgotten.
What staff should and should not do	Ensure that all staff know the procedures even if they do not have any direct tasks
How the systems will be backed up (including what will be backed up, how often and which media will be used)	Ensure that regular backups are taken. Decide where the backups will be stored and which media will be used to store the data e.g. cloud, magnetic tapes.
A timeline to establish how quickly the systems will need to be backup and running	After a disaster not all operations will be needed immediately. A plan should be made to define how long the organisation can be without each system. Critical systems must be identified and will need to be recovered first.
An alternative location for operation (hardware, software and personnel).	After disaster the organisation may need to move quickly to another location. Hardware, software and personnel should also be available (along with the backups) so that the organisation can function again quickly.

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B3 – Policy Passwords

Key Vocabulary	
Parameter	A parameter is a set of rules to be followed or behaviours that need to be demonstrated.
Default password	A password that is automatically allocated when your account is set up. Users are always advised to change default passwords on first use.

Password Policy

Organisations that take data security seriously usually have a comprehensive password policy that they ask employees to follow.

This policy usually covers the creation and protection of passwords.

Passwords should be suitably complex. Ccomplexity is increased by:

- Greater password length
- Combination of upper and lower case characters, numbers, punctuation and other symbols
- Passwords SHOULD NOT use words found in a dictionary, familiar names (family or pets) or be easy to crack
- Using initial letters from a memorable phrase, mixing lower and upper case letters and numbers

Protection of Passwords:

Passwords are out first point of defence for our files and personal information.

Usually an organisation's software will prevent the creation of passwords that:

- Don't match the organisation policy, have been used before or are in a dictionary.

Password Strength	Description	Examples
Weak	An obvious password using either standard letters or numbers, often personal to the user (e.g. family name, birthday) so can be easy to guess	PASSWORD,123456
Medium	Uses a combination of letters and numbers, but could use more special characters and less recognisable words to make it more difficult to guess.	LiverPool5
Strong	Makes use of special characters, numbers and upper/lower case letters, making it very difficult to guess.	A?vEr8gS!

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B3 – Policy Security Policies

Key Vocabulary

Software Audit	A manual or automated process that lists the name, version and installation date of all software found on a digital device. The process may be carried out remotely, for example, across a network, or in person.

Acceptable Use Policies

Unapproved software could contain malware that might infect the organisation's systems and network.

It may conflict with the hardware or other software on the digital system.

An acceptable software policy explains what will be done to help prevent any attempted installation and use of unapproved software.

Use of unapproved software

The use of unapproved software is usually disallowed by an acceptable software policy. Breaching the policy may result in disciplinary action e.g. verbal or written warning even if the employee did not install the software.
Most operating systems can prevent the use of certain software applications.
Preventing the use of unapproved software helps to protect the organisation from malware and potential external threats.

The AUP reinforces the need for the installed software to be used responsibly and legally.
It also usually prohibits unauthorized duplication of the software for home use unless permitted by the software's licence.

Installation

- Users are usually forbidden from installing unapproved software or updates.
- Users may ask for approval for new software or be asked to select from an approved list.
- Users may need support from their manager or another department for their request to be considered.
- Users will need to justify why this new software is required for their job.

Security policy statements may state the following:
You may ***not*** install software on digital systems used within the organisation.
All software requests ***must*** be justified and approved by a manager and then sent to the IT department or Help Desk in writing or by email.
New software ***must*** be selected from the IT department's approved software list unless no match can be found that meets your needs.

Enforcing AUPs

The operating system applies the safeguards that prevent the installation of software if the user does not have sufficient administrative rights.

Other techniques that prevent unwanted installation of software:
- CCTV monitoring of employees
- Software audit of digital systems

Example Exam Questions:

1. Identify the risks of installing and using unapproved software.

2. Describe how an acceptable software policy might be enforced.

3. Describe what a software audit is.

4. Give two reasons why employees are not automatically allowed to duplicate software for home use.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim B Cyber Security – B3 – Policy Actions after and Attack

Key Vocabulary	
Data Protection Controller	The named person in an organisation who takes responsibility for the safety and security of the organisation's data.
Remedial Action	An action taken to fix something that has gone wrong; a remedy

Actions to take after an attack

After an attack it is crucial that an organisation and its employees have a clear idea of the actions to take to resolve the situation and reduce the likelihood of it happening again.

•1. Investigate → •2. Respond → •3. Manage → •4. Recover → •5. Analyse

Investigation

The organisation will investigate the nature of the attack. It will want to find out the following:

- **The type of attack** e.g. malware, network attack, data theft, phishing
- **The severity of the attack** e.g. Level 1 (low risk) to Level 5 (severe risk
- **Which processes or services are affected**.
- **When it happened**.

The information gathered at this point is vital to help the organisation determine how to respond, manage and recover from the incident.

Response

The type of response will vary depending on the severity of the attack.

An organisation will inform:

- Stakeholders (employees, shareholders, customers, suppliers, business partners etc)
- Appropriate authorities (law enforcement including police, National Crime Agency, **Data Protection Controller**, etc)

Notifying stakeholders

This is important as data breaches might include confidential details (usernames and passwords) that customers might use for other services.

Informing stakeholders may lead to a damage to public image.

Not telling the authorities could result in legal action and potential fines.

It is also important that interested parties are kept updated as more information becomes available from the investigation.

Manage

The priority is to isolate the problem by containing the threat as close to the source as possible.
e.g. disconnecting an infected computer from the network or blocking unauthorised network traffic by using a firewall.

Recover

The organisation will have a separate disaster recovery policy that it will follow in the event of an attack.
This will include:

- Employees responsible for specific tasks
- The expected timeline
- The **remedial action** involved.

Analyse

Analysis will focus on the following:

- What went wrong,
- How it happened (internal or external threat),
- How it could have been prevented,
- How effectively the organisation responded to the attack
- What lessons have been learned.

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C1 - Responsible Use: Sharing Data

Key Vocabulary	
GPS (Global Positioning System)	A navigational system that uses data transmitted by satellites to calculate the location of the GPS-enabled device.
Data Subject	An individual whose personal data is being stored.

Accessing Shared Data

Mobile devices can be used to share information about you, such as your location e.g. social media check ins

Think carefully about allowing your technology to reveal where you are.

Generally, you should switch off your location settings for your protection.

The real-time geo-data from your smartphone/device is used to track your location via GPS so you can share it. This enables you to find places of interest near by.

This data is used by organisations to:

- Send you adverts for things close to where you are
- Provide relevant travel updates

Location based services also provides security and fraud prevention as your location can be matched to where your bank card is being used. If the 2 don't match, someone else may be using your card without your knowledge.

Cookies

Web applications often use session cookies to keep a user logged in, even if they leave a page and return to it later.

Cookie data is used by organisations in many ways e.g. sharing data that enables a server to deliver web content that is tailored to your needs.

Transactional Data

Many things you do generate transactional data e.g. buying something, using a bus ticket or adding a diary entry.
Data that is generated by one part of an organisation is almost always used by another part.

Sales data might be analysed so that manufacturing can be adjusted.
Stock data might be analysed so that anything not selling well can be sold at a discount.
Staff holiday information could be used to plan manufacturing.

Using shared data responsibly

It's important that data is shared & used responsibly. Individuals & organisations should act in ways that ensure the use of data meets legal & ethical requirements.
Legal – The Data Protection Act sets out the requirements to protect data. (Became the General Data Protection Act (GDPR) in May 2018). Failure to protect data may result in a heavy fine.
Privacy – Duty of confidentiality in the UK which reinforces our right to privacy. Personal information is protected under the law. E.g. Medical conditions
Ethical – Organisations should ask for permission from the **data subject** to share the information.

Benefits of using shared data	Drawbacks of using shared data
Sharing diaries helps teams to coordinate activity	Users must make sure that they are not breaching any copyright
Collaborating on projects means more ideas	Data must be protected by law
Work can be shared in real time, so projects can be completed more quickly.	Data can be sabotaged by damage or changed
Sharing music on a family network means you only pay once	Sometimes data gathered for one reason might notbe entirely relevant in a different context
Using existing data reduces the costs of collecting new data	Data moving from one system to another can lose integrity
More information means better decisions	Data must be downloaded from trustworthy sources to make sure it is not infected

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C1 - Responsible Use: The Impact of Technology and the Environment

Key Vocabulary	
Consumables	Items such as ink cartridges, paper, toner, cleaning products, maintenance tools and cables.
Motherboard	The main electronic circuit board that all the other computer components, such as memory, processor, graphics card etc., plug into

The impact of technology on the environment

The technology we use everyday impacts on the environment in many ways e.g. the use of non-renewable resources:

- precious metals used in manufacture of technology,
- coal used to generate electricity to power technology
- old technology that requires special disposal.

Making, using and disposing

Manufacturing and using computer technology generates waste products.

- A computer can contain up to 2kg of lead, which is a poisonous metal.
- Copper is used in computer cables, it is becoming increasingly rare and more valuable.
- Using a desktop PC uses an average of 200 watts
- Using a laptop PC uses an average of 80 watts

Consumables

Disposing of computers and their **consumables** should be taken seriously as it is important to limit the use of non-renewable resources.

The disposal of computers and other electrical products is governed by law.

Upgrading and Replacing

Organisations need to decide whether to upgrade or replace their technology when it slows down and reaches the end of its useful life.

Two possible solutions:
Replacing components e.g. Replacing memory will make the computer run faster

Replacing the whole system - tends to be done when it would be more expensive to replace all the necessary components.

Benefits of technology	Drawbacks of technology
Electronic communication can mean less paper and ink are used. Reduces the number of trees that need to be cut down.	Digital devices consume electricity when they are in use and when they are recycled . This means increased burning of fossil fuels.
Digital devices can be used to monitor the environment, enabling better weather predictions.	Old computers are not always easy to disposeof. Parts are not always recycled, resulting in more waste going to landfills.
Industrial processes can be computer controlled rather than human controlled, which is more efficient and less polluting.	Some countries illegally send waste to third world countries. People in these countries are exposed to toxic substances when trying to extract the metals.

Usage and Settings

Usage settings can be adjusted to help reduce the impact of technology.
1. Use auto power-off setting on your computer
2. Use power saving settings on devices to reduce screen brightness.
3. If you don't really need to print a hard copy of a document then don't.

Benefits of Technology			
Technology	**Benefits for organisations**	**Benefits for individuals**	**Benefits for society**
Email	Fast communication with customers and other stakeholders	Faster and cheaper than letters, no need to find a post box and it is easy to include photographs or other images with no printing required.	Easier to keep in touch with friends and family in a way that is not restricted by time (as phone call would be if contact lived in another time zone).
Online information	Competitor information e.g. pricing is easily accessible. It is easier to stay up to date with relevant regulations and laws	Research is much easier with more information at your fingertips, which has a positive impact on education	Access to a wide variety of information and online courses.
Online shopping	Brings an organisation's products and services to a wider market	Convenience for individuals who can shop 24/7 and access a wider range of products and services. Often means more competitive prices.	An online business does not require the same financial model as a high street business and can be easily set up.
Online chat	Many organisations approve of office-based chat systems which staff can use to ask each other questions and share information	Online chat brings people closer together and can help those who are lonely.	Chatting online helps build communities and enables people in society to find and connect with others who share similar interests.
Media access and download facilities	Access to libraries of images, animations,music and video footage that can be used in marketing campaigns.	Downloading media, such as music and games, at any time of day and is sometimes cheaper than what you would pay in a shop	Accessibility to worldwide media and internet radio from around the world in addition to the usual paid for download services.

Example Exam Question

TechnoWhizz are considering the following projects to improve their use of digital systems:

- Project 1: Providing all employees with new devices for accessing and using the cloud services.
- Project 2: Power off all systems outside working hours
- Project 3: Distributing internal documents using only electronic methods.

(d) Evaluate the risks each project would have to Technowhizz and which project would have the most positive impact.

(9)

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C2 – Legal and Ethical: Legal Requirements and Professional Guidelines

Key Vocabulary	
Discrimination	The unfair treatment of individuals (or groups) based on factors such as race, age, gender or disability.

Legislation	Professional Guidelines	Accepted standards
•Laws are created to make individuals or groups behave in a specific way. •They are updated and reviewed regularly. •Laws are enforceable. •If you break a law you could be punished with disciplinary action, be fined or even imprisoned.	•Professional guidelines are usually focused on a single professional. •Guidelines are based on actions that have been agreed by the key organisations or sectors bodies. •Only enforceable if a 'licence' to practice is involved e.g. medical licence can be withdrawn •Organisations that do not follow professional guidelines risk their reputation.	•These are ways of doing things that are generally agreed to be examples of best practice. •They are often developed over time and can be influenced by a range of factors, such as emerging technologies. •They are not enforceable by law.

The Legal Requirements

In the UK there is a range of legislation that organisations must observe in relation to **discrimination.**
Organisations that discriminate can be prosecuted under the law.
Legislation that could impact an individual's ability to access information and services includes:

- Race relations regulations.
- Equality laws.
- Discrimination legislation.

Ways in which access to services or information could breach legislation include:

- Provision of web content that could be considered offensive to a group or individual,
- Failure to provide accessibility tools for an employee,
- Provision of content in a format that is not accessible to some groups or individuals.

The **Web Accessibility Initiative (WAI)** is a family of standards that includes the four principles of **WCAG (Web Content Accessibility Guidelines)** that focus on access to information and services in relation to web content.

Four Principles of WCAG:	
Perceivable	The user should be aware of the content through their senses
Operable	The user must be able to interact with and operate the interface in some way.
Understandable	The user must be able to understand the operation of the interface and the information it contains.
Robust	Must be robust and able to cope with a wide variety of users accessing it using assistive technology

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C2 – Legal and Ethical: Net Neutrality

What is Net Neutrality?

Net neutrality is your ability to pick any available products or services that you choose without your choices being filtered or influenced by the organisation that provides your internet connection.

The connections used to navigate the internet are provided as a service by various ISPs.
A basic principle of the internet is that all data is treated equally. This means that ISPs do not block, tamper with, speed up or slow down any data transfers based on source, destination or type of internet data.

The UK

In the UK different IPS are able to offer a range of packages that limit overall internet speeds.

These ISPs cannot actively prioritise speeds for certain types of data (e.g. streaming video services) or block access to rival websites because they have been paid to do so by a commercial competitor.

ISPs cannot charge customers more for accessing particular websites.

The positive/negative impact of net neutrality on organisations

Good

- Better and more reliable services may be possible
- ISPs could subsidise free internet for more people from greater profits
- Block illegal use of pee-to-peer (P2P) technologies which allow sharing of copyrighted material
- ISPs can charge content providers more for resource-hungry traffic e.g. gaming, video etc., allowing more investment in their network

Bad

- User choice may become limited e.g. search results filtered to clients paying ISPs
- Smaller organisations may not be able to compete or innovate with larger rivals
- Free speech through social networking could be blocked or filtered
- Greater monitoring of users' online activities, sold to advertisers etc.

Example Exam Question

TechnoWhizz wants to introduce a video streaming service to provide content for their devices.

(b) Describe how 'Net neutrality' will help TechnoWhizz compete with more established video streaming services.

(3)

Acceptable Use Policies (AUP)

Most organisations create and enforce an acceptable use policy (AUP).

The AUP is designed to outline the ways in which an IT system can be used.

The AUP also provides a list of restrictions and potential sanctions that can be applied if the rules are broken.

AUPs can apply to internal users or external customers.
An AUP will also cover employees accessing an organisation's network remotely.

The purpose of an AUP

- An AUP is a key part of an organisation's information security policy.
- It is one way of reducing internal and external threats.
- The AUP document acts as both a set of guidelines and a warning.

Benefits of AUPs	Drawbacks of AUPs
Users know what is expected of them and if they sign it then they have agreed to follow the code of conduct.	Users may not like the introduction of a new code of conduct as they may find it restricting.
It holds users accountable for their actions and acts as a contract for disciplinary action when users have not followed it.	Users may feel that you do not trust them if you set out exactly everything they can and cannot do.
It is more likely that users will use the network for more legitimate purposes.	An AUP is a voluntary agreement and therefore has no legal standing.

Contents of an AUP	
Scope	•States who the document applied to e.g. employees, customers etc. •States what the document covers. •States when the policy came into effect.
Assets	•States what is covered by the document e.g. equipment, documents, email communication •Often includes sensitive business information and intellectual properties.
Behaviours	•Acceptable behaviours that an organisation might expect from its employees, e.g. honesty, loyalty, collaboration, respect of peers. •Unauthorised behaviours that the organisation does not want e.g. harassment, attempts to gain unauthorised access.
Monitoring	•How the organisation monitors employee behaviour. •Monitoring may be electronic e.g. electronic passes, internet history, CCTV footage
Sanctions	•How the organisation deals with breaches of AUP •Should define the processes and potential sanctions that can be applied. These may be minor (e.g. verbal/written warning) or in extreme cases, termination of employment or legal action.

An AUP must have a section confirming that the employee/customer has read the policy and agrees to its rules.
Some organisations may include inappropriate use of social media in their AUP as an unacceptable behaviour.

Use of social media for business purposes

- Social media is a popular method for organisations to advertise their products and services.
- Businesses may use **third party cookies** or paid advertising to target users that have visited similar sites or used search terms related to that type of business.
- Social media platforms, e.g. Facebook, allow businesses to run promotions to their users.
- These are very effective as they precisely target the right audience.
- Video bloggers may be paid to promote certain products as part of their presentations.
- They are required to acknowledge that they are being promoted by businesses to do this.
- This endorsement is often very influential.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C2 – Legal and Ethical: Data Protection Principles

Data Protection Principles

- The Data Protection Act – protects your information and the way information about you is used.
- May 2018 - the GDPR (General Data Protection Regulations) were introduced that manage the way data is captured, processed, stored and protected.
- The GDPR has led to additions to the principles of the Data Protection Act.

Benefits of data protection	Drawbacks of data protection
Those who break the data protection laws face going to prison or paying a fine.	Data protection laws are difficult to enforce. Lots of similar organisations hold personal information but do not always follow data protection laws.
Individuals now have rights over the data that organisations store about them.	Conviction rates are low, which indicates the organisations are breaking data protection laws without being prosecuted.

Capturing Data

- Data must only be captured for a specified purpose.
- Data must be adequate and relevant *and limited to only what is necessary* in relation to the purpose for which it was collected.
- Data must be accurate and kept up to date *with errors quickly erased or rectified. It must be easy for data subjects to withdraw consent*

Processing Data

- Data must be processed in line with the rights of data subjects.
- Data must be processed fairly and lawfully *and in a transparent (clear) way.*
- Data captured for one purpose must not be used for a different purpose.
- *Data must be processed in a secure manner.*
- *Data belonging to EU citizens must be processed in line with a GDPR even if the organisation processing the data is not in the EU.*

Penalties and Actions

Breaching the requirements of the GDPR can result in a fine of up to 4% of the organisation's turnover, or up to €20 million.

Storing and Protecting Data

- Data must not be kept for longer than is necessary.
- Organisations must take appropriate action to prevent unauthorised or unlawful processing of data.
- Organisations must act to prevent accidental loss, destruction or damage to data.
- Data must not be transferred to another country that does not have adequate protection legislation to protect data.
- Individuals have the right to find out what data is being stored about them *and the right to find out whether data is being held about them and where and why this is occurring.*
- *If data has been breached organisations will have to notify customers of the breach within 72 hours.*
- *All data being stored about individuals should be anonymous, unless knowing the identity of the data subject is necessary to make sense of the data.*

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C2 – Legal and Ethical: Data and the use of the Internet

Key Vocabulary	
Digital Footprint	The trail you leave when you visit different sites on the internet. You can view your footprint by visiting the browser history section of your browser.

Data and the use of the internet

Organisations have a responsibility to ensure they behave in a legal and ethical fashion.

The growth of the internet has challenged the idea of personal privacy and users often leave a much larger **digital footprint** than they imagine.

The right to be forgotten

The 'right to be forgotten' is a legal concept.
It means the individual is free to pursue their life without being treated unfairly because of a specific action taken or comment made in their past.
The EU has adopted the 'right to erasure' of data.
This can result in an individual asking an organisation to remove any copies of, or links to, information held about them.
Organisations should tell third parties who may also have copies or links to erase them.
Large fines can be applied if the organisation's data controller is not seen to have all reasonable steps to meet this requirement.

Appropriate and legal use of cookies and other transactional data

Using online services results in a user leaving a digital footprint.
This digital footprint often contains personal information that organisations could sell to other organisations.
This data could then be used to support targeted adverts.
This data can be stored and accessed in several ways.

Cookies

A cookie is a block of data stored temporarily in the memory of the user's device OR for longer periods in a text file.
Cookies were created to legitimately store memorable data about a user's interactions with a website e.g. user preferences, contents of shopping basket.
These are often called **first party cookies** as they are used and created by the same website domain and are generally seen as harmless.
Third party cookies are cookies that can be used by advertisers – these track online activities and display advertising offers reflecting browsing habits and core interests.
These cookies can be blocked or deleted to preserve a user's privacy
The ePrivacy Directive (aka the '**cookie law**') requires that users give consent before a website can store and access information on their personal device. This usually appears as a cookie consent banner on the organisations website's main

Transactional Data

Organisations also collect transactional data, which is stored digitally.

e.g. an online purchase would include:
- personal information,
- delivery address,
- item details,
- date and time of purchase,
- a unique order ID,
- tracking data for delivery.

This data also has to be stored and processed legally and ethically.

Example Exam Questions

PublishShare is a publishing company.

The company uses a range of digital systems to support its business.

(a) Explain how PublishShare could personalise advertisements for its customers when they are visiting their website.

(2)

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C2 – Legal and Ethical: Intellectual Property

Key Vocabulary	
Trademark	The recognisable design, words or symbols that have been legally registered by a company or individual for a company, product or name.
Patent	The exclusive rights granted to a person or organisation for a specific idea, design or invention.
Copyright	A legal right protecting the use of your work. There are different rules about how and when your work could be used and how long copyright is retained.
Plagiarism	Copying someone else's work or intellectual property without acknowledging them, claiming it as your own.

Intellectual Property

Intellectual property (IP), includes brand names, logos and product designs.

There are 3 common ways organisations can protect their intellectual property to prevent other organisations using them:

1. Registering a **trademark**,
2. Applying for a **patent**,
3. By **copyrighting** it.

Intellectual property applies to anything:

- That is copyrighted,
- That is trademarked,
- That is the subject of a patent.

Copyrighted materials can be identified by the © symbol.
Trademark materials can be identified by the ™ symbol.
Patents are rights given to a product that has been invented.

During the **life** of a patent no other person or organisation can replicate the product. Once the patent has expired, other businesses can copy the product.

Commonly protected property includes:

- Music
- Artistic works
- Logos
- Inventions
- Designs
- Discoveries
- Literature and other publications
- Software/programming code

When the patent is registered a search is made to make sure that the idea has not already been patented.

Plagiarism

Plagiarism is copying the answer for a question from the internet or a book without saying that it is a direct copy
You must say exactly where the information has come from.

- Acknowledging text from a book: (author, year of publication, name of publication, name of publisher).
- From the internet, you should include: (author (or 'unknown' if not known), date accessed, URL of the website).

Chocawoca is a confectionary manufacturer that makes high quality sweets and chocolates that they sell in their shops and online.

Chocawoca's recipes are protected by intellectual property rights.

(a) Explain how **one** method of intellectual property rights protection will help Chocawoca protect its recipes.

Example Exam Questions (2)

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C2 – Legal and Ethical: The Criminal Use of Computer Systems

Key Vocabulary	
Peer to peer (P2P)	A way of explaining two systems that are connected and have the same rights and privileges.
Cracks	Comes from the expression 'crack the code'. This is usually a software program that removes the need to register the software to be able to use it.

4 main areas of common criminal activity using computing systems

Area	Activity
Unauthorised access	Criminals target a system and identify its security weaknesses. They then access the unsecure system to identify a profile they can use and change the privileges to give them better access to the system
Unauthorisedmodification of materials	Criminals who have managed to access a system to find content to change. They change files, such as documents, web pages, or download files to give them access to other systems, or divert money to other bank accounts.
Creation of malware	Malware, such as viruses, is written by criminals to be used to infect systems, either to cause damage or to steal money or information. The malware can be modified to take different actions on different systems after it has infected them.
Intentional spreading of malware	Malware is spread through infected files. The files can be spread via the internet or USB devices. Often, malware is spread through user ignorance.

How malware can be spread

Because most malware infects and duplicates silently on a computer system, many users do not know their computer system has become infected and will unknowingly pass the malware onto another user, for example, by sharing infected files.

Popular routes for spreading malware include:

- Social networking sites
- Internet chat rooms
- Infected websites
- Illegal **peer-to-peer** (P2P) network downloads of copyrighted material
- Use of software '**cracks**' to illegally register commercial software
- Email attachments
- Following malicious links.

Malware is usually spread through users unknowingly downloading and opening infected files and having insufficient protection on their computer system.

The most common pattern of infection:

- User clicks a link
- Infected file is downloaded
- Infected file is opened by the user
- Malware activates quietly and infects other files on the computer system
- Malware takes action e.g. deleting files, sending infected emails, encrypting files for ransom etc

Example Exam Questions

1. Give the four most common criminal uses of computer systems.
2. Describe how malware can be spread.
3. Give at least 3 popular routes for spreading malware.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim Planning and Communication in Digital Systems – C1 – Forms of Notation: Information and Data Flow Diagrams

Presenting Information

Information may be presented in a number of different ways:

- Written descriptions
- Tables
- Charts
- Diagrams
- Storyboards
- Infographics
- Dashboards

Data Flow Diagrams

A data flow diagram shows:

- Who or where the input data comes from
- How data flows around the system
- How the data is processed
- What data is stored
- Who or where data from the system is output to.

A person, organisation or another system which sends or receives information

A process or function, sometimes but not necessarily numbered

A file or database

Data or information flow shown by the direction of the arrow

Information Flow Diagrams (IFDs)

IFDs show how information flows through a system or organisation including:

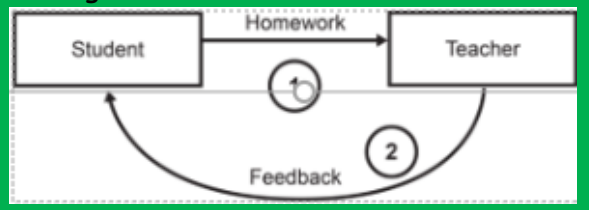
- People / users of the system
- How information flows between organisations and how information flows between different areas of an organisation

How to create IFDs

Use squares for key parts of the system such as people or departments.

Use arrows to show how the information flows around the system

Label the arrow with what information is being transferred

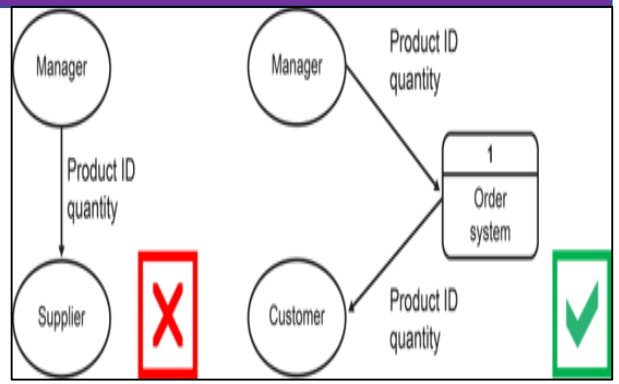


To create a data flow diagram:

- Identify the **process** and the **entities** shown in the data flow diagram (DFD)
- Label the data flows

Points to note when creating data flow diagrams:

- You should never draw a data flow line between two entities
- Data flows always go to, or come from, a process
- A process box needs at least one input and at least one output
- Do not draw a data flow from an external entity directly to or from a data store
- Numbering process boxes may be useful if you need to refer to the processes
- Data stores can also be numbered. D can also be used for a digital store and M for a manual store



CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim Planning and Communication in Digital Systems – C1 – Forms of Notation: Flowcharts

Flowcharts

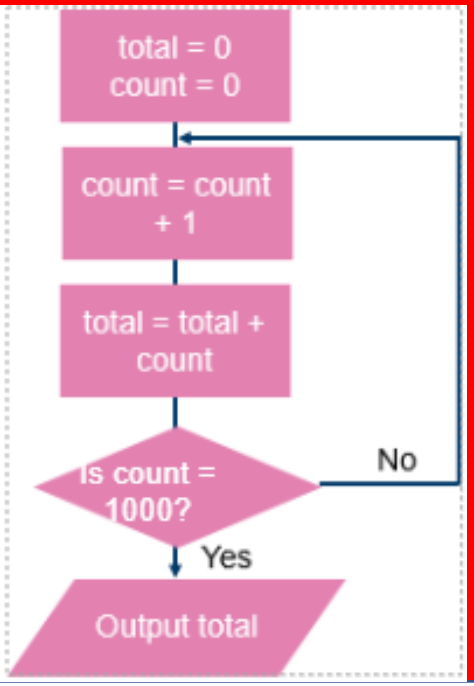
A flowchart is often a clearer way to present the steps required

They are easy to understand

They are less likely to be misunderstood than a list of text

Counting in a flow chart

The statement count = count + 1 means "Add 1 to the variable called count"

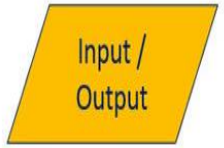


Flowchart Symbols

Terminator
Used to represent the Start and end of a program with the Keywords BEGIN and END.

Decision
Used to split the flowchart sequence into multiple paths in order to represent SELECTION and REPETITION.

Process
An instruction that is to be carried out by the program.



Input / Output
Used to represent data entry by a user or the display of data by the program.

Arrow
Indicates the flow of the algorithm pathways.

Subprogram
References another program within the program.

Real uses for flow charts

Companies will often create flowcharts to show what to do when a problem occurs, such as:

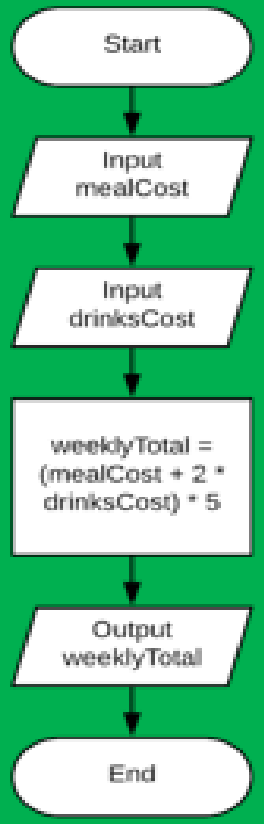
- Fire procedures
- Customer complaints
- Manufacturing defects
- Companies may also have procedures to help employees to do their day to day work

Variables in a flow chart

Variables allow us to store a number or text in a flowchart

Variables are often used in calculations Calculations will always be in a process box

You can input or output what is stored in the variable



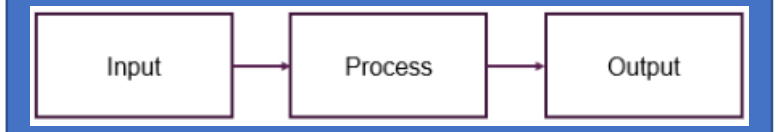
BTEC DIT Component 3 Knowledge Organiser

Learning Aim Planning and Communication in Digital Systems – C1 – Forms of Notation: Systems Diagrams

Computer Systems

A computer system consists of all the hardware and software required to perform the required tasks

At its simplest, a computer system consists of input, processing and output



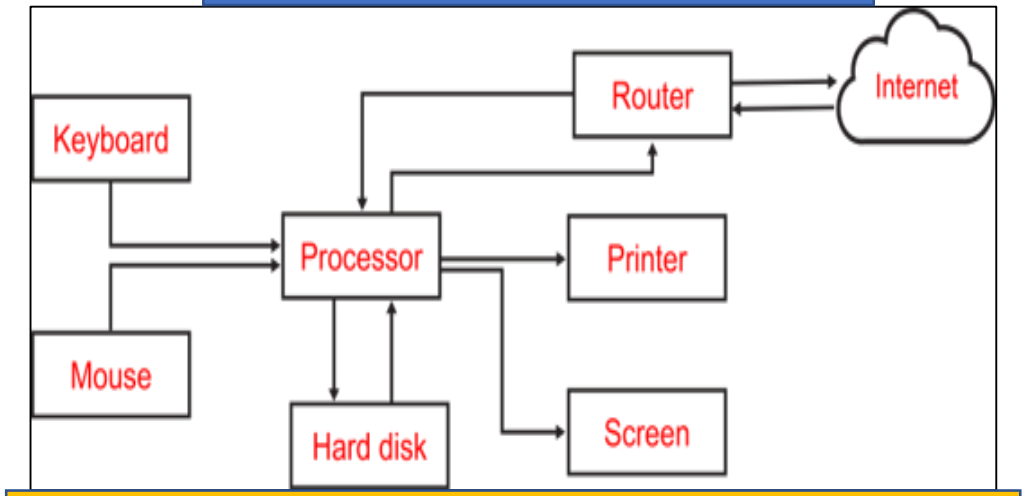
Drawing a systems diagram

Most IT system diagrams will include:

- Hardware
  - Input / output devices
  - Storage devices / databases
  - Network equipment such as Wi-Fi access points
  - Computers / Smartphones / Tablets
- People involved in the system can also be included
- Processes or events are described

Step 1: Identify the key components
Step 2: Draw the key parts
Step 3: Connections
Step 4: Label the diagram

A Simple System Diagram



Why use system diagrams?

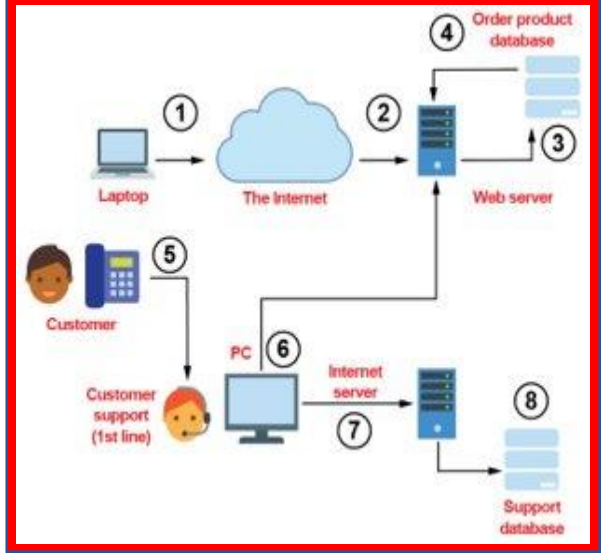
- They can give a lot of information in a small space:
  - Input and output devices
  - Connections between components and data or signals
  - Computers / servers involved
  - Communication devices
  - Feedback loops
- They are a good way to communicate designs, infrastructure and processes about IT and an organisation's systems
- They help in designing workable systems

Other uses for Systems Diagrams

System diagrams can also be used for an organisation

System diagrams may use standard icons or be more informal

You may choose to just use boxes with text inside



CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim Planning and Communication in Digital Systems – C1 – Forms of Notation: Tables and Written Information

Written information

Written information is good for giving further analysis of data.

Uses in business

- Policies
- Catalogues
- Reports
- Emails
- Letters

Rules on writing:

- Write concisely
- Use appropriate language for your audience
- Check your writing for spelling, punctuation and grammar
- Include references and acknowledgements

For long documents or business reports:

- Include page numbers and a contents page
- Include a summary

Tables

Tables are a useful way of presenting information How the data is presented in a table makes a difference to how easy it is to extract useful information

Uses of tables:

- Timetabling
- Financial models
- Planning
- Survey results
- Flight departures / arrivals

Disadvantage:

A table may not be able to show all the required information

TIME	DESTINATION	FLIGHT	GATE
12:39	LONDON	BA 903	31
12:57	SYDNEY	QF5723	27
13:08	TORONTO	AC5984	22
13:21	TOKYO	JL 608	41
13:37	HONG KONG	CX5471	29
13:48	MADRID	IB3941	30
14:19	BERLIN	LH5021	28
14:35	NEW YORK	AA 997	11
14:54	PARIS	AF5870	23
15:10	ROME	AZ5324	43

How to improve table design:

Giving the table a title

- Referencing the source of the data
- Including units for the speed
- Considering what data the audience needs
- Use formatting features to help the reader:
  - Conditional formatting makes it easier to see the difference in speeds
  - Bold column titles are clearer

Example Exam Question

4.A coffee shop chain is currently researching when their shops have the most demand from customers. They will be using this information to work out how many baristas they need to employ at any given time.

Their research will be presented as a report to the board of directors to help them make decisions.

(a) Describe **three** features that could be used in the report to make it easier to read.[6]

(b) As part of the research, a large amount of data has been found which shows how many customers use the shops in each hour they are open. This data will be presented in a table.

Describe **two** guidelines for creating a useful table.[4]