CHURCH STRETTON SCHOOL

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.

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

Learning Aim C The Wide Implications of Digital Systems – C1 - Responsible Use: Equal Access to Information and Services

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)

sky Virgin media BT EE TalkTalk

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)

CHURCH STRETTON SCHOOL

BTEC DIT Component 3 Knowledge Organiser

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

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.

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*

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.

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

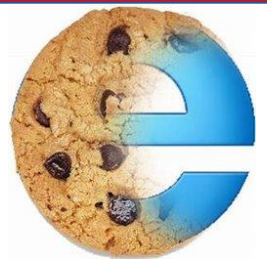
The 'right to be forgotten' is a legal concept.
It means the individual is free to pursue their life without being treated unfairly because of a specific action taken or comment made in their past.
The EU has adopted the 'right to erasure' of data.
This can result in an individual asking an organisation 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).

Example Exam Questions

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.

(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

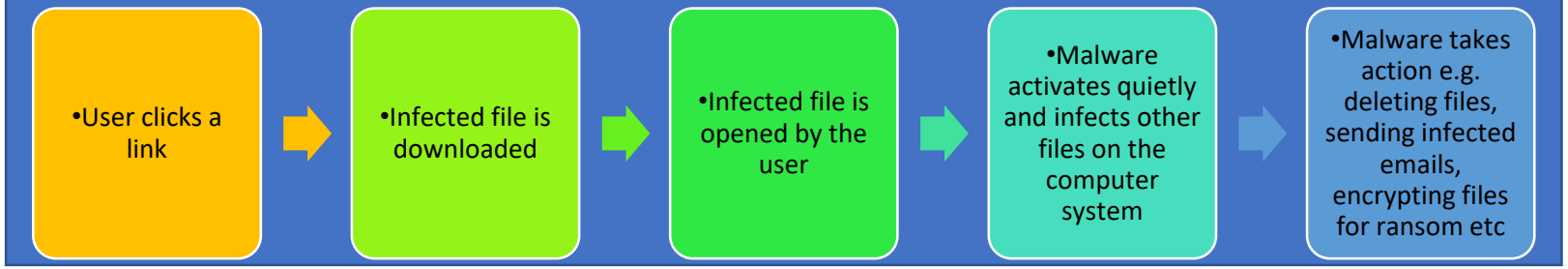
Because most malware infects and duplicates silently on a computer system, many users do not know their computer system has become infected and will unknowingly pass the malware onto another user, for example, by sharing infected files.

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:



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.