Cambridge (CIE) IGCSE ICT

Your notes

Safety

Contents

Physical Safety

What is physical safety?

- Physical safety is **creating a safe environment when using technology**
- It includes **considering dangers** that could lead to **serious injury or loss of life**
- Identifying **strategies to mitigate** dangers
- Safety risks include:
  - **Electrocution from spilling drinks near electrical equipment**
  - **Fire hazard from overloading plug sockets**
  - **Equipment overheating**
  - **Trailing cables (trip hazard)**
  - **Heavy equipment falling and causing injury**

Risk	Cause	Prevention
Electrocution	▪ Spilling drinks near electrical equipment	▪ Keep liquids away from electrical equipment
	▪ Touching live cables	▪ Ensure that cables are properly insulated and protected ▪ Use **non-conductive** materials where possible ▪ Ensure that electrical equipment is **turned off** and **unplugged** before cleaning or maintenance ▪ Use **circuit breakers** or **fuses** to prevent electrical overload

Fire hazards	▪ Sockets being overloaded	▪ Use surge protectors to prevent electrical overload ▪ Ensure enough plug sockets in the room ▪ Don't plug too many devices into the same plug socket ▪ Don't leave devices plugged in and unattended
	▪ Equipment overheating	▪ Ensure that equipment is properly ventilated and not obstructed ▪ Keep flammable materials away from heat sources ▪ Regularly check equipment for signs of wear or damage ▪ Use fire extinguishers in case of emergencies ▪ Turn off or unplug devices when away from the location ▪ Do not cover any air vents on devices
Trip hazard	▪ Cables not properly secured or organised	▪ Use cable ties or clips to secure cables ▪ Keep cables away from areas where people are walking ▪ Secure cables where you can, like under desks to stop protruding into open areas ▪ Use cable covers to protect cables and prevent tripping hazards ▪ Regularly inspect cables for signs of wear or damage ▪ Where possible use wireless devices to reduce cables
Personal safety	Improperly secured equipment	▪ Ensure that equipment is properly secured and stable ▪ Regularly check the stability of locations containing devices
	Equipment not placed on stable surfaces	▪ Keep equipment away from edges and other potential hazards

Your notes

		▪ Regularly inspect equipment and locations containing devices for signs of wear or damage

Worked Example

Using computers can lead to several physical safety issues.

Describe four of these types of issues.

[4]

Answer

Electrocution, caused by touching bare wires / allowing food and drink to spill liquids onto computers [1]
Falling objects can cause injury [1]
Tripping over loose cables can cause injury [1]
The fire is caused by overloading power sockets / overheating computers [1]

Data Protection

What is the Data Protection Act?

- The Data Protection Act (**DPA**) is a law that **protects personal data** from being misused
- Examples of personal data would include
  - **Name**
  - **Address**
  - **Date of Birth**
  - **Race**
  - **Religion**
- Most people that store personal data has to follow the Data Protection Principles although there are a few exemptions:
  - **Domestic purposes** – if you only use personal data for such things as writing to friends and family or taking pictures for your own enjoyment, you are not subject to the DPA
  - **Law enforcement** – the Police investigating a crime is not subject to the DPA. E.g. if someone has been suspected of a crime they can't request to see the evidence about them
  - **Intelligence services processing** – personal data processed by the intelligence services (e.g. MI5) is not covered by the DPA

The data protection principles

Principle	**How does it affect a company?**	**Example**
1. Personal data must be fairly and lawfully processed	A company has to be clear about what personal data they wish to collect and what they want to use it for	A school can request personal data to be able to call guardians in an emergency
2. Personal data must be collected for specified and lawful purposes	A company cannot use personal data for any purpose other than what they stated originally. They also cannot pass this data on without permission	A company asks for a phone number to call regarding delivery but then uses it to market new products

3. Personal data must be adequate, relevant and not excessive	A company cannot request personal data that they do not need right away	A bank cannot ask for their customer's previous trips when opening an account
4. Personal data must be kept accurate and up to date	If a company holds personal data that is wrong or out of date then you have a right to have it corrected or deleted	If a bank has a customer's old address then they will not be able to send up to date statements
5. Personal data will not be kept for longer than is necessary	A company must delete personal data once they no longer have a need for it	If a customer closes their account the company must delete their data
6. Personal data must be processed in line with people's rights	If requested a company must provide a customer with all the personal data they hold on them	A hospital has to give a patient's full records if requested by the patient

Personal & Sensitive Data

What is personal data?

- Personal data is any **data that can be used to identify an individual**
- Example of personal data include:
  - **Name**
  - **Address**
  - **Date of birth etc.**

Personal data	**Description**
Personal name	Refers to the **full name** of an individual, including their **first name** and **last name**
Address	The **physical location** where an individual **lives**, including their house **number, street name, city, and postal code**
Date of birth	The specific **day, month, and year** when an **individual was born**

Gender	The individual's identity relating to male, female, don't know, prefer not to say
Personal images (e.g. a photograph in school uniform)	An image of an individual **wearing their school uniform**, which can be used to identify and locate them.
Payment details	**Bank card details** used for purchasing items or **bank details** to access online banking
Passwords	The **combination of letters, numbers and symbols** used to access accounts that are held by the individual

Why should personal data be protected?

- **Inappropriate disclosure** of personal data can **lead to privacy breaches, identity theft,** or **misuse of the information**
- Personal data could be **sold to third party companies**
- Individuals could be **held to ransom** over **personal data gathered**
- **Information gathered** could be used to commit a **physical crime**

How to avoid data being inappropriately disclosed

- Personal data must be kept **confidential** and **protected** through **privacy settings** on websites such as **social media** or **strong passwords** on websites where personal data is held or used
- Access to personal data should be **limited to authorised individuals**
- **Think before you post –** consider what information could be gathered from your image or content
- Check website details about the **collection**, **storage**, and **use** of **personal data**
- Only access websites where personal data is used or viewed when on a **secure, encrypted** connection

What is sensitive data?

- Sensitive data is **subset of personal data** that **if disclosed could lead to personal harm**
- Sensitive data **requires stricter protection**
- Examples of sensitive data include:
  - **Ethnic or racial origin**
  - **Sexual orientation**
  - **Medical history etc.**

Sensitive data	Description
Medical record/history	Information related to an **individual's health**, including any **past illnesses, medical conditions, or treatments they have received.** This can include any genetic or DNA information about **genetic characteristics**
Political views	The individual's **opinions on political matters/issues** and how they are being handled by the current **government.** This can include **memberships in political parties**
Ethnic/racial origin	The **ethnic or cultural origins** of the individual's ancestors
Criminal activities	Any **past or current criminal offences**
Membership of trade union	Made up of workers to **protect and advance the interests of all workers in the workplace**
Sexual orientation	Defining who you are **attracted to**, the opposite gender, the same gender, or to both or more than one gender
Biometric data	**Body measurements** used to identify us uniquely like **fingerprints** or **facial features**

The Need for E-Safety

What is the need for e-safety?

- E-safety is about **knowing about** and **using** the **internet safely** and **responsibly**
- It refers to when an individual is **using** the **internet**, **email**, **social media**, **online gaming**
- E-safety refers to the individual **knowing** how to **protect** themselves from **potential dangers and threats**

Need	Description
Protects personal information	Awareness that personal information should not be shared freely
Prevents cyberbullying	Awareness of how to act online and how to avoid falling victim, creating a safe and respectful online environment
Guards against online scams	Identify and avoid online scams, phishing attempts, and fraudulent websites that may try to trick them into sharing personal or financial information
Ensures digital reputation	Mindful of online behaviour and interactions, protecting your digital reputation, which can have long-term consequences in personal and professional lives
Promotes privacy and control	Have control over privacy settings on social media platforms, allowing a limit to who can access/view personal information and posts
Prevents exposure to inappropriate content	Avoid encountering explicit or harmful content online, reducing the risk of exposure to inappropriate material or online predators
Secures online gaming experiences	Engage in online gaming responsibly, avoiding sharing personal details and maintaining respectful behaviour towards other players
Guards against malware and viruses	Protecting devices from malware, viruses, and other online threats, preventing data loss, privacy breaches, or device damage

Promotes responsible digital citizenship	Develop responsible online behaviours, promoting respectful conduct while interacting with others on the internet
Supports overall well-being	Maintain a healthy balance between online and offline lives, reducing the risk of addiction, mental health issues, or negative impacts on relationships and self-esteem

Your notes

Using IT

How can you be safe using IT?

- There are many ways to remain safe when using technology, **by following the advice and guidance** users can stay safe whilst:
  - **Using the internet**
  - **Sending/receiving email**
  - **Using social media**
  - **Playing games online**

Task	Advice & guidance
Using the internet	▪ Use **trusted websites** recommended by teachers or reputable sources ▪ Utilise **search engines** that only allow access to **age-appropriate websites** and use **filters** to ensure **inappropriate content** is not seen ▪ **Never** reveal **personal information**
Sending/receiving email	▪ Be aware of the **potential dangers** of **opening** or **replying** to **emails** from **unknown** people, including **attachments,** potential dangers include **phishing, spam** ▪ Ensure you know **who the email is for** when considering **sending personal data** or **images** via email, only with **people you know** and **not with identifiable content** like school photos
Using social media	▪ Know how to **block** and **report** people who send content or messages that are **unwanted** ▪ Know where the **privacy settings** are to reduce the number of people who can see your posts or images ▪ Be aware of the potential dangers associated with meeting online contacts face to face, **do not meet anyone you do not know**, if you do, take an adult and meet publicly

Your notes

	▪ **Do not distribute** of **inappropriate images** and **inappropriate language** ▪ **Respect the confidentiality** of **personal data belonging to other people** ▪ **Only accept friend requests** from **people you know** ▪ **Parents should be aware of what you are doing online**, discuss what you are doing online ▪ **Do not post images** or **details** that can be **used to locate you**
Playing games online	▪ **Do not use real names** as usernames ▪ **Never share personal** or **financial details** with **other players** ▪ Know how to **block** and **report players** for **inappropriate messages or comments**

Worked Example

A student uses social media to keep in contact with other people.

Describe four strategies that the student could use to stay safe when using social media to communicate with others.

[4]

Answers

Four of**:**

Don't give out other people's personal information such as address or phone number [1]
Don't send inappropriate images to anyone [1]
Don't open/click on suspicious links/adverts on social media [1]
Don't become online 'friends' with people you do not know//don't contact/chat with people you do not know [1]
Never arrange to meet someone in person who you only met online [1]
If anything you see or read online worries you, you should tell someone about it/block them [1]
Use appropriate language [1]
Set security so only friends can contact you [1]