# AQA Computer Science GCSE

## 3.8 Ethical, legal and environmental impacts of digital technology on wider society, including issues of privacy

Advanced Notes

This section explores the ethical, legal and environmental impacts and risks of digital technology on society. It also covers data privacy issues and the cultural implications of technology.

Exam questions for this topic are typically (though not always) essay questions, worth around 9 marks. Exam questions will be taken from the following areas:

- cyber security
- mobile technologies
- wireless networking
- cloud storage
- hacking (unauthorised access to a computer system)
- wearable technologies
- computer based implants
- autonomous vehicles

Before exploring some of the principles and questions around this list of areas, here are some of the general considerations that are taken into account.

## Cultural issues

Cultural issues arise from the differences in moral values between people based on their values, traditions and beliefs. For example, in the UK, people are generally happy for photographs containing them to be taken in public and shared online. In other countries, this would not be seen as acceptable. When creating a new computer system, computer scientists must consider where their system is going to be used and what people's attitudes towards it would be to ensure it is inclusive.

## Legal issues

Computing technology is covered by several laws in the UK. Although specific knowledge of these laws is not required, it is helpful to be aware of some examples.

### Data Protection Act 2018

Data protection legislation governs how organisations (including businesses, charities and government departments) can use the personal information of individuals. In the UK, data protection is governed by the Data Protection Act 2018.

Personal information / data: any data that can be used to identify an individual. For example, their name, address, date of birth, phone number.

Anyone who uses personal data must make sure that it is:

- Stored securely
- Used fairly, lawfully and transparently
- Stored for no longer than is necessary
- Kept accurate and up to date

Everyone has rights in relation to their personal data, including:

- The right to be fully informed about how their personal data is being used
- The right to request access to the personal data that an organisation holds about them
- The right to have their personal data erased
- The right to request that an organisation stops processing their personal data

**Computer Misuse Act 1990**

The Computer Misuse Act 1990 aims to prevent unauthorised access to or modification of data. It lists the following offences:

- Unauthorised access to computer material.
  *For example: You notice your sibling has written their username and password down in a notepad. You use their login details to access their laptop and read their private emails without their consent.*

- Unauthorised access with intent to commit or facilitate commission of further offences.
  *For example: You guess your colleague's password and log in to their online banking. You then transfer money to your own account without their knowledge.*

- Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer.
  *For example: You send a virus as an email attachment to a rival business's computer system, knowing it will slow their operations, hoping to give your company an advantage.*

- Unauthorised acts causing, or creating risk of, serious damage.
  *For example: You break into a hospital's computer system as a prank, not realising that your actions would crash the server and delay patient records being accessed in emergencies.*

- Making, supplying or obtaining anything which can be used in computer misuse offences.
  *For example: You write the code for a phishing website that mimics a bank's login page, intending to collect other users' login details, even if you haven't shared the code with anyone or put the website onto the internet.*

## Environmental issues

Environmental issues refer to the impact that computers and digital technology have on the natural world. This includes the energy used by devices and data centres, the limited natural resources that are used during the manufacturing of hardware, and the problem of electronic waste (e-waste) when devices are thrown away. Many computers contain harmful materials that can damage the environment if not disposed of properly (e.g., lead and mercury).

Technology can also help the environment, for example it reduces paper usage by enabling electronic communications to be used instead, such as emails.

## Data privacy issues

Most citizens normally value their privacy and may not like it when governments or security services have too much access. Governments and security services often argue that they cannot keep their citizens safe from terrorism and other attacks unless they have access to private data. Citizens have data privacy rights that are defined by law, as outlined in the legal issues section of these notes.

## Specific examples

You will be expected to understand the general principles behind these issues rather than have detailed knowledge from specific issues. In many cases, there is no right or wrong answer, so you should discuss the general principles that apply, and explain some of the different issues and points of views that people may have.

### Cyber security

Cyber security is explained in more detail in Topic 6: Cyber security. It consists of the processes, practices and technologies designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

***Issues:***

- How can cyber criminals be identified when they mostly operate online and use sophisticated methods to stay anonymous?
- Law making can be a lengthy process, can legislators keep up as technology progresses?

### Mobile technologies

Mobile technologies include smartphones, tablets, and other portable devices that allow users to communicate, browse the internet, and access apps from almost anywhere. These devices are now a central part of daily life, often storing personal data and linking to cloud services.

***Issues:***

- Can apps track user locations without consent?
- Are users aware of how much data is collected by installed apps?
- Do constant notifications and large amounts of screen time affect mental health?

### Wireless networking

Wireless networks, such as Wi-Fi and mobile data connections, allow devices to connect to the internet or each other without physical cables. They provide convenience, especially in homes, schools, and public places.

***Issues:***

- How secure are public Wi-Fi networks from hackers?
- Are users always aware of who controls the network they connect to?
- Whose responsibility is it to keep data secure - the network operator or the person using it?

### Cloud storage

Cyber security is explained in more detail in Topic 4: Computer systems. Cloud storage allows users to save data on remote servers instead of local devices. This makes it easier to access files from anywhere and share them across devices or with others.

***Issues:***

- Who owns the data once it is stored in the cloud?
- Could cloud storage providers share or sell data?
- What happens if the cloud service suffers a data breach?
- Are users always aware of where their data is physically stored? If it is in a different country, then could the laws regarding data protection be different, putting their privacy at risk?
- What are the consequences if a cloud provider shuts down suddenly?

### Hacking (unauthorised access to a computer system)

Hacking refers to gaining access to a computer system without permission. It is discussed in more detail in Topic 6: Cyber security.

***Issues:***

- Are organisations doing enough to protect systems from hackers?
- Could stolen data be used for identity theft or blackmail?

**Wearable technologies**

Wearable technologies include devices like smart glasses, wearable cameras, and fitness trackers that are worn on the body. They often track health and activity data and can interact with smartphones or other systems.

***Issues:***

- How securely is the wearer's personal data stored or transmitted?
- Could employers or insurance companies misuse health data?
- Could wearable cameras be used to invade others' privacy?

**Computer based implants**

Computer-based implants are electronic devices placed inside the human body, often to support medical functions, such as heart pacemakers or brain implants.

***Issues:***

- What if the implant malfunctions or is hacked remotely?
- Who is responsible if an implant causes harm - the developer or doctor?
- Should people be forced to get implants for health reasons?

**Autonomous vehicles**

Autonomous vehicles, also known as self-driving cars, use sensors and AI to drive without human control.

***Issues:***

- Who is legally responsible if a self-driving car crashes?
- Can the software be hacked to cause accidents or steal vehicles?
- How do autonomous vehicles make moral decisions in accidents - for instance, should they be programmed to continue course to injure several people, or to swerve and injure less people?