1.6 Ethical, legal, cultural & environmental impacts of digital technology

1.6.1 Ethical, legal, cultural & environmental impact

This section looks at the impact of digital technology on our lives from different perspectives.

Digital technology can mean computing devices that you use such as a laptop, mobile phone or smart watch - but it can also be larger systems such as CCTV, online databases, social media and even pandemic virus tracking applications.

Considerations

In the last few decades, computer science has massively changed every aspect of our society. Jobs have been lost in many industries, and in some cases have been made completely obsolete. There are also many new industries that did not exist before computers, and the situation is changing and evolving all the time.

When we look at the impact of computers and computing technology, there are certain areas that we should consider:

Ethical issues are about what would be considered right and wrong by society.

Legal issues are about what is actually right and wrong in the eyes of the law

Cultural issues are about how groups of people with particular beliefs, practices or languages may be affected e.g ethnic groups, religions, countries.

Environmental issues are about how we impact on the natural world:

- The impacts of Computer Science on the Environment are both positive and negative

- Computers have helped in manufacturing, engineering, surgery, medicine etc.

- However, generally technology requires electricity to function

- Often judgements need to be made as to whether this is a good balance

- Also, what happens to old computers/robots etc?

Privacy issues concern how our personal information is kept safe, and how we have a right to privacy.

Ethical Issues

Stakeholders

A stakeholder is a person who may be involved either directly, or indirectly with an issue or problem. Most issues and problems will have many stakeholders, some may be obvious, some may be less obvious.

Questions about ethical, legal, cultural, environmental and privacy issues often carry high mark allocations. To gain the higher band of marks you should be able to identify more than just the 'obvious'

Ethical issues are about what would be considered right and wrong by **society**. If a computer system enables the users to do things that most people disagree with but are not necessarily breaking any laws, then that may mean that the practice is unethical.

Ensuring Public Safety

Ensuring public safety is paramount. As new technologies are introduced, they bring safety concerns.

For example, driverless cars may soon be on the roads in the UK. The designers of driverless cars have not only had to ensure the safety of passengers, but also of other drivers and pedestrians. Ethics apply here as a situation may occur where the car's **software** has to decide who has safety priority, the passengers or other road users.

Data Security

Personal data is precious and needs to be kept safe. Unfortunately, there are people that attempt to hack systems in order to gain access to other people's data. Social media accounts, phone mailboxes and networks that computers connect to are all prone to hacking.

Some people may also use **malware** to obtain data. Recent times have seen the increased use of a type of malware known as **ransomware**. People who write ransomware do it to extort money from unsuspecting users. Once the ransomware infects a computer it encrypts data on it, denying users access unless a ransom is paid.

1.6 Ethical, legal, cultural & environmental impacts of digital technology

1.6.2 Legislation Relevant to Computer Science

As Computer Systems become not only more advanced, but also much more widespread in our lives, people will no doubt think of ways of using the computer systems to exploit others and gain an unfair advantage. Laws will be developed to make it illegal to do this, but there will always be a delay and the legislation is bound to be out of date.

Governments that create the laws may also be poorly advised, and lacking the understanding of the issues - they may often apply completely unsuitable restrictions to computer systems based on how society has behaved before the systems were developed.

For your exam, you need to understand several key pieces of legislation.

The Data Protection Act 2018

The Data Protection Act has been around for several decades, but was updated in 2018 to include the General Data Protection Regulations (GDPR). The DPA concerns how personal data is stored and maintained. There are six principles you need to know:

1. Data should be processed fairly and lawfully: not obtained by deception, and the purpose clearly stated.

2. Data should only be used for the purpose specified.

3. Data should be relevant and not excessive.

4. Data should be accurate and up-to-date.

5. Data should only be kept for as long as necessary.

6. Personal data must be handled in a way that ensures security.

Computer Misuse Act 1990

The Computer Misuse Act is often referred to as the "hacking law". It makes it an offence to access a computer system without authorisation. Accessing a computer system may just be logging on as another user because they have shared your password, or could mean a much more complex attack on a computer or network using sophisticated techniques (this is the kind of attack that you would see in a movie!)

- It is illegal to access **data** stored on a computer unless you have permission to do so. Unauthorised access is often referred to as **hacking**.

- It is illegal to access data on a computer when that material will be used to commit further illegal activity, such as fraud or blackmail.

- It is illegal to make changes to any data stored on a computer when the user does not have permission to do so. If you access and change the contents of someone's files without their permission, you are breaking the law. This includes installing a virus or other **malware** which damages or changes the way the computer works.

Copyright Designs and Patents Acts 1988

The Copyright, Designs and Patents Act gives everyone rights over any original work that they create. When someone writes a new piece of text, song, creates a video, or designs something, then they are said to be the copyright holder of the work. Other people are not allowed to copy the work (which is said to be intellectual property), without the permission of the copyright holder.
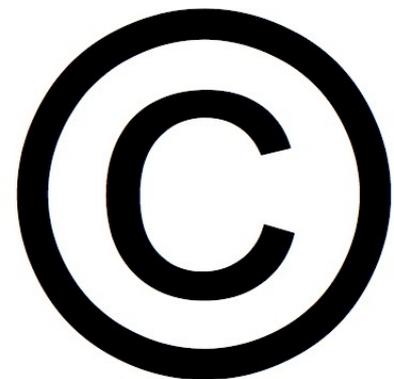
When a new idea needs a more formal protection, the owner can apply for a patent. The owner will need to prove that the idea is unique and will register the design with the patent office. If the idea is particularly good and may be worth a lot of money, then this may need to be done in many different countries, which can be very expensive.

The patent will apply for a set term, usually several decades. Some of the larger tech companies hold a vast number of patents ranging from the shape of a mobile phone, to some speculative ideas that it would not be possible to implement now. If technology

developed in such a way that the patent design could actually be made, then a royalty fee would have to be paid for every product which used it.

Software Licenses (Open Source and Proprietary)

One way to classify **software** is through ownership and **licensing**. There are two types of ownership and licensing software:

- open source software

- proprietary software

While both types of software are usually widely available, they differ quite considerably in what can and cannot be done.

Open source software

Open source software is software that is free of **copyright**.

Open source software has several advantages:

- It costs nothing and provides the **source code** so that anyone can modify the software for their own purposes.

- It can have many authors. This enables programmers to contribute to the development of a program over time, refining and improving it and adding extra features.

- A modified version, known as a **derivative**, must also be made freely available for anyone else to use or adapt.

Open source software has its disadvantages too:

- There is no guarantee that it works properly as there is no requirement for anyone to ensure it is **bug** free.

- Support might not be readily available, especially if the program is not in widespread use.

Examples of open source software include:

- Linux operating system

- Firefox **web browser**

- Python programming language

- Open Office productivity **suite**

- Thunderbird **mail client**

- Apache **web server**

- GIMP image editing software

- Moodle virtual learning environment

Proprietary software

Proprietary software is software that is copyrighted, which means it can only be obtained by paying for a licence.

Proprietary software has many advantages:

- The product should be free of bugs. If bugs still exist, updates known as **patches** are often provided free of charge, which fix these bugs.

- Help can be sought from the organisation who supplied the software if problems occur.

- Feature updates which extend the software's facilities are often available, although usually at a cost.

- Proprietary software that is in widespread use often has support available from many sources.

Proprietary software also has a number of disadvantages:

- There is an initial or ongoing (subscription) cost.

- Software cannot be adapted to meet the needs of the user. Only the **machine code** version of the software is distributed, which cannot be edited.

- It can be limited to a single computer or **network**, so unless the licence allows it, a user may not redistribute the software.

Examples of proprietary software include:

- Windows and OS X operating systems

- Microsoft Office productivity suite

- Adobe Creative Suite productivity software

- Logic music creation software

- paid-for games for consoles