Moral, Ethical, Legal and environmental impacts of digital technology on society

Ethical – Ethics are rules developed by society that are imposed on an individual. For instance, most organisations including you school will have a code of conduct of IT usage for teachers and pupils

Moral – Is an individual framework for understand the difference between right and wrong. For instance many people choose to make their code free in order to improve society, but it is still not unethical to make money from writing computer code

The Ten Commandments of Computer Ethics (From the Computer Ethics Institute)

Thou shalt:

1. not use a computer to harm other people
2. not interfere with other people's computer work
3. not snoop around in other people's computer files
4. not use a computer to steal
5. not use a computer to bear false witness
6. not copy or use proprietary software for which you have not paid (without permission)
7. not use other people's computer resources without authorization or proper compensation
8. not appropriate other people's intellectual output
9. think about the social consequences of the program you are writing or the system you are designing
10. always use a computer in ways that ensure consideration and respect for other humans

Environmental Impacts

- The disposal of computer waste is a big problem because they contain many toxic chemicals. Often old computing equipment is illegally shipped for disposal to developing countries.
- The growth in cloud computing means a greater need for storing data online. For this data centres are used but they require huge amounts of electricity, thereby contributing to climate change.
- Cobalt is a key element requited for Lithium batteries for powering mobile devices. Much of the World's cobalt is mined in the Congo even by very young children in appalling conditions.

Environmental benefits

- Less reliance on paper saving resources
- More opportunity for online global communication and collaboration thereby saving on travel and associated pollution
- Greater insight of environment and climate through using computer to model and analyse and process environmental data

Legislation

Computer Misuse Act (CMA)
The purpose of the CMA is to prevent:

- unauthorised access to computers by hackers
- intentionally impairing the operation of computer systems through denial of service (DOS) attacks on web servers or distributing viruses
- the theft of data

Three levels of offence:

1) Unauthorised access
2) Unauthorised access with intent to commit an offence
3) Unauthorised modification of data

Copyright, Designs and Patents Act (CDPA)

Copyright is a law that protects the creators of original pieces of work. No one else has the right to use or copy it without permission from the owner. This ensures that people can be rewarded for their work.

Plagiarism To pass off some else's work as one's own work.

Patent An inventor has the exclusive right to create, use and sell an invention for fixed period

Piracy Illegally copying and distributing copyrighted material.

Fair use allows copyrighted work to be used legally in certain situations

- personal or educational use (not commercial use)
- use only a small amount of the work (e.g. a short quote)
- acknowledge original source of the work

Copyleft work can be copied, modified used even used for commercial gain as long as the derived works are also distributed under copyleft.

Creative Common Licences (CCL) The creator of the work has explicitly given anyone permission to use the work.

Investigatory Powers Act This is legislation that allows public authorities to carry out mass surveillance on electronic communications.

Justification - By monitoring electronic communications security services can keep us safe from terrorists and other serious criminals

Concerns - Can infringe on our privacy and civil liberties

In a liberal democracy there will always a need to balance security and privacy, but where we draw that line will always be a matter of debate.

Some powers of the security services under the IPA

- can hack into computers, networks, mobile devices, servers
- internet service providers have to store which websites users visit for 12 months and allow access to authorities when requested
- carry out mass surveillance of communications; authorities can collect bulk data including data about people who are not suspected of anything.
- demand that an internet service provider and other companies provide access to a customer's communications including keys to encrypted data

General Data Protection Regulation (GDPR)

The purpose of the GDPR is to ensure that personal information collected by businesses and other organisations are protected.

Personal data is defined as anything that allows an individual to be identified (e.g. name, biometric data)

Six principles of the GDPR
Personal information must:

- be used fairly and lawfully
- be used only for specific purposes for which it was collected
- be adequate, relevant and not excessive
- be accurate and kept up to date
- be kept for longer than is necessary and deleted when it is no longer needed
- be kept secure against unauthorised access

Other aspects of the GDPR

- The data subject needs to be notified if their data are shared with other organisations
- Obtain consent from the data subject to their process data
- Obtain consent from parents or guardians to process children's data.
- Allow data subjects to have their data removed
- Allow data subjects to access the data held about them
- Pay big fines for a breach of the GDPR

Challenges facing legislators

- Technology can be used for illegal purposes in unforeseen ways. And because technology changes rapidly the law cannot keep up with these changes.
- Internet is global, so any activity that may be legal in one country may be illegal in another.
- Encryption allows the monitoring of criminal activity much more difficult.
- Crimes may be committed by states
- Powerful technology companies lobby for their own interests