4.8 Consequences of Uses of Computing

Moral Issues

Example: A social media company uses an algorithm that keeps users scrolling for longer, even though it may negatively affect their wellbeing. The moral issue is whether it is right to prioritise profit and engagement over users' mental health.

- Who could be helped or harmed by the technology?
- Is the decision right or wrong, even if it is legal?
- Are people being treated fairly and respectfully?
- Could the technology negatively affect wellbeing, privacy, safety, or freedom?
- Is profit, efficiency, or convenience being prioritised over people?

Ethical Issues

Example: A company collects large amounts of personal data to train an AI system. The ethical issue is whether users have given informed consent and whether their data is being used fairly and responsibly.

- Has personal data been collected and used fairly?
- Have users given informed consent?
- Is the system biased against certain groups of people?
- Is the technology transparent, or are decisions hard to understand?
- Could the organisation be using technology in a way users would not expect?

Legal Issues

Example: A business stores customer details but fails to protect them properly, leading to a data breach. The legal issue is that the business may have broken data protection law, such as the Data Protection Act or UK GDPR.

- Which laws or regulations might apply?
- Has personal data been stored, processed, or shared lawfully?
- Could copyright, licensing, or intellectual property rules be broken?
- Has the organisation followed its legal responsibilities for security?
- Could someone face fines, prosecution, or legal action?

Data Protection Act

- Protects personal data about living individuals.
- Organisations must collect, store and use data fairly, lawfully and securely.
- People have rights over their data, such as knowing how it is used and asking for it to be corrected or deleted.
- In exam answers, link this to privacy, consent, security, data breaches and misuse of personal information.

Copyright Act

- Protects original work such as software, music, films, images, books and website content.
- Makes it illegal to copy, share, download or use copyrighted material without permission or a licence.
- Helps creators control how their work is used and allows them to be paid for it.
- In exam answers, link this to software piracy, illegal downloads, plagiarism and licensing.

Computer Misuse Act

- Makes unauthorised access to computer systems illegal.
- Covers hacking, accessing data without permission, spreading malware and changing or damaging data.
- Also covers creating or supplying tools that could be used for computer misuse offences.
- In exam answers, link this to hacking, malware, denial-of-service attacks, unauthorised access and cybercrime.

Regulatory Investigative Powers Act

- Regulates how public bodies and authorities can carry out surveillance and intercept communications.
- Covers monitoring emails, phone calls, internet activity and encrypted communications in certain situations.
- Aims to balance crime prevention and national security with people's right to privacy.
- In exam answers, link this to surveillance, monitoring, encryption, privacy and government or police investigations.

Cultural Issues

Example: A website or app is designed only for English-speaking users and does not consider different languages, customs, or accessibility needs. The cultural issue is that technology may exclude some groups or fail to respect different ways people communicate and use digital services.

- Does the technology work well for people from different backgrounds?
- Are language, customs, beliefs, or local expectations considered?
- Could the design exclude or disadvantage certain communities?
- Is the technology accessible to people with different needs?
- Could it change how people communicate, learn, work, or behave?