**P3 - Use of Information**

Information can be a powerful tool, so there are some laws that govern its use. These include the Data Protection Act (1998), the Freedom of Information Act (2000), and the Computer Misuse Act (1990)

**Data Protection Act 1998**This act governs the use of information about individuals. Anyone who processes personal information must register with the DPA registar and follow eight laws, which state that information must be:

* Fairly and lawfully processed
* Processed for limited purposes
* Adequate, relevant and not excessive
* Accurate and up to date
* Not kept for longer than is necessary
* Processed in line with your rights
* Secure
* Not transferred to other countries without adequate protection.

These laws ensure people are not harmed by misuse of personal information. TelX must comply with the Data Protection Act, as it stores information about all of their employees.

**Freedom of Information Act**The Freedom of Information Act is about access to official information. It gives individuals or organisations the right to ask for information from any public authority, including central and local government, the police, the NHS, colleges, and schools. They then have 20 days to provide the information requested. They may refuse if the information is exempt from the Act. Examples of exemption are if releasing the information could prejudice national security or damage commercial interests.

**Computer Misuse Act**As most information is now stored digitally, it is important that there are laws regarding the use and access of digital information. The Computer Misuse act makes it illegal to:

* Access any computer program or data without permission – the most common form of this is using someone else’s user ID and password
* Gain unauthorised access to a computer system, regardless of intent
* Modify computer contents without permission. This means impairing the operation of a computer, a program, or the reliability of data. It also includes preventing access to any program or data. Examples of this are the introduction of a virus, modifying or destroying another user’s files or changing financial or administrative data.

The act also makes DOS and DDOS attacks (spamming a server with dummy requests to overload it in order to prevent people from accessing to information, and commercially damaging the target system) illegal.

**Ethical Concerns**  
When dealing with computer misuse and access to information, it can be difficult to distinguish between whether something is truly harmful. For example, the Freedom of Information act exists to give everybody access to information, which is a basic human right. However, distinguishing between public and private information is more circumstantial. For this reason, it is illegal to request information about individuals without their consent, as this would constitute a violation of privacy.  
On the other hand, sometimes access to this sort of information is required and seems fair, such as by somebody researching their family history, or the police going through personal data to convict a criminal. These types of cases cannot be classified by law alone, as they involve ethics.  
It is for this reason that the Computer Misuse Act makes it illegal to access a computer system without permission, *regardless of intent.* This massively clarifies cases where the defendant claims they did not have malicious intentions, and protects people’s privacy.

**Organizational policies**As well as laws, most organizations will have codes of conduct to outline how their computer systems can be used. These rules generally cover Email (No threatening, harassing or spam emails), Use of internet (accessing banned sites).  
These codes of conduct generally protect ‘whistle-blowers’ (those who draw management’s attention to other misusing computer facilities), such as IT technicians and network administrators, who are usually the first to spot misuse.