**P3 - Use of Information**

**Legal issues**

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 systems without adequate protection

These laws ensure people are not harmed by misuse or mishandling of personal information.

**M2**  
TelX must comply with the Data Protection Act, as it stores information about all of their employees. If it does not, then they may face large fines.

**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.

**M2**TelX can make use of this act if it needs information from a public authority. Additionally, others can request (limited) information about TelX from public authorities.

**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
* 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 or network with dummy requests to overload it) illegal, in order to prevent people from denying others access to information.

**M2**The IT technicians and network administrators will need to enforce these laws and maintain security across their computer systems. Failure to comply with this can result in damage to systems, loss of data, and the exposure of confidential information.

**Ethical issues**

**Organizational policies**As well as laws, most organizations will have codes of conduct to outline how their computer systems can be used.

**Email**Policies will ban threatening, harassing and spam email. They usually allow for limited personal use.

**Use of Internet**  
Accessing blocked, illegal or gambling websites is against nearly all policies. Some personal use is allowed, as its difficult to tell apart from professional use, such as googling something, or checking a site during a lunch break.

Policies will usually protect ‘whistle-blowers’, those who expose others breaching the code of conduct, usually IT technicians or network administrators.

The policy is usually determined by the nature of the business or organisation. An organisation with a hierarchy that operates on a need-to-know basis will usually have policies restricting access to information, with strict rules about who can access information and how it is stored.

A decentralised organisation will restrict access to information physically, as servers and storage facilities will be offsite.

**M2**TelX’s policies will affect all of its employees, as they have to follow the policies. TelX will also need systems and staff in place to know if anyone breaches the policy.

**Operational issues**

**Security of information**  
Although organizations have rules, it is the job of the IT and network staff to enforce them. This includes restricting access to some data, logging who has accessed or modified data, and alerting management to anyone breaking the rules.

Small organisations have looser policies, partially because there are less staff (sometimes only one) to enforce them.

Larger organisations will have much more complex rules, usually decided by the IT department and management.

**Backups**Any storage medium can - and eventually will - fail. Therefore, it is important to have backups – redundant copies of information. In IT, this involves copying important data (such as the contents of fileservers) to another storage medium. This can be done on-the-fly (every time a modification is made), or on a schedule.  
It is also important to practice a recovery from the backup, to ensure it is working properly.

**M2**TelX will likely need to invest in a server/s to store all of the logs and data, as well as to ensure there is a way to enforce computer system policies.

They will also need backup storage and a reliable method of performing backups and restores. They could buy their own servers, or hire servers from a cloud computing company.