P3

Data protection act

The Data Protection Act is a law designed to protect personal data stored on computers or in an organised paper filing system.

Businesses, organisations and the government use computers to store information about their customer’s clients and staff in databases. For example:

* Names
* Addresses
* Contact information
* Medical history etc.

Principles

1. Data is to be used fairly and lawfully
2. Should be used for limited specifically stated purposes
3. Used sufficiently, relevant and not excessive
4. Data should be accurate and kept up to date
5. Personal data should be kept for any longer than is necessary
6. Data shall be processed and handled according to the data protection rights
7. Should be kept securely and should be safe
8. Should not be transferred outside of the UK without adequate protection

Freedom of information act

The freedom of information act handles access to official information. It allows people and organisations rights to ask for information from public authorities which includes central and local government, the police, NHS, colleges and schools. The authorities then have up to 20 days to provide the information that has been requested. They’re able to refuse if the information is exempt from the act, for example if the information released could prejudice national security or commercial interest, then that is exemption.

Computer misuse act

* Unauthorised access to computer programs or data – this is when someone has used another user’s ID and password (without permission) to access programs and data
* Unauthorised access intending to commit a serious crime
* Damaging the process of a computer program or the reliability of data and stopping access to computer programs and data. This goes along with installing viruses, destroying another user’s files or altering with financial or administrative data

Codes of practise

Organisations would have a code of practise to clarify what uses can be made of their computing facilities.

* Use of email – emails that are threatening or harassing are banned along with spamming emails.
* Use of the internet – using the internet to access sites that have to do with pornography or gambling are banned by the code of practise or by filtering software.
* Whistle blowing – codes of practise would usually protect computer users who attract managements’ attention to others users’ misuse of the system

Organisational policies

The policies that an organisation may have could have an effect on how their information is treated. An organisation with a tough hierarchy that functions on a need to know basis is likely to impose policies restricting access to information. For example the organisation may keep its databases, files and email servers in a secure central data centre.

Information ownership

The department that produces data should own every field of data in every record. They have the responsibility for making sure that the data produced is entered into the computer system in a timely way and that it is accurate and consistent.

Security of information

System users trust the IT department to keep its information secure so that it is safe from unauthorised access, alteration or even destruction. It is under the management’s responsibility to specify who is able to look at the information and who is able to update it. Other organisations have much more complex rules such as requiring a log of who has accessed information and who has made updates to information.

Backups

In case of physical or processing problems, it is a good idea to backup information frequently. It could be a full backup of all information or a partial backup of just the information that has been changed since the previous backup. IT departments should occasionally run-through a recovery or restore from the full backup of all the information then apply any partial backup to make sure it works.

Health and safety

There are procedures that apply to screens and monitors – how they are positioned and how they are used. Keyboards, mice, chairs and tables must all be properly positioned for example chairs should be positioned appropriately so it can be suitable for the user. Computer users are entitled to eye tests. They should have regular breaks away from the computer so they can relax their eyes.

Organisational policies

Organisations usually have policies for the use of information systems that their staff has to follow. These could range from keeping information private within the company to the procedures to follow for correcting any information that appears to be wrong.

Business continuance plan

IT is the most important part of a business continuance plan (BCP) so organisations can figure out a strategy of how operations can continue if any major part of an it system should fail. IT departments ought to have things set up so if there is ever a major failure, they will be able to carry on providing service, even though a more limited one. An example is to have a dual network set up, having alternate terminals attached to each network. If one network fails, then half of the other terminals will continue to work.

Costs

It’s important to manage costs of an IT system. There are two important areas that should be considered when costing an IT project:

* Additional sources required – when a new system is introduced, it often entails one-off costs of new equipment purchase and installation along with user training and testing. There are more recourses needed in an IT department therefore there will be ongoing costs in order to run a new system.
* Cost of development – when the system is running, there will be ongoing costs for minor changes so that the system is kept in line with the organisation’s needs.

Impact of increasing sophistication of systems

Systems today are becoming increasingly sophisticated and need the following:

* More trained personnel – users often require training in order to use equipment, basic computer features, processes brought in with new computer system and transactions, queries and also reports that form the new system.
* More complex software – Modern development software hides a lot of complexity from the application builder and so this means that the focus on business problems that new systems will solve and create overall better and more complex systems. But if problems occur, development software experts and a business software expert would be required to fix the problem.

M2

As data is to be used fairly and lawfully and kept secure, being a HS Smith worker, you are not obliged to give out any personal details stored within the business. Data should be locked away on a password protected computer and all filing cabinets should be locked away. If done without consent this breaches the Data Protection Act. There will be consequences such as being given a warning, or even being let go and it could also affect the company making the company look bad and unprofessional. Natural consequences would be getting charged and sent to prison for up to 6 months and issued a fine.

The freedom of information act may handle access to official information, although other organisations and people are able to request information stored within the company (HS Smith) as a worker you should consider up to 20 to be able to provide the information requested. If not done so, complaints will arise and it will affect the company making the company seem as if they do not know how to run their own business. The freedom of information act should be handled by making sure all information is private and should not be altered by anyone. Consequences could be that if not handled well you could be issued a fine and charged with 5 months of prison.

If there is an issue that files under the Computer Misuse Act such as unauthorised access intending to commit a serious crime, this could affect HS Smith very badly. The company would have to find out who has committed the crime and charge them but also would have to apologize on their behalf to whoever has been affected by the crime. The computer misuse act should be handled in a way that when using the internet, access to inappropriate websites should be blocked and computers should be highly password protected. User’s should send a reduced amount of emails and should be told not to spam. Also people should not still be in the building using computers after hours set. Consequences would be that whoever commits the crime would be charged up to 5 years in prison and would be charged with a fine.

Using the company’s computers to access websites such as for gambling or trying to access pornography websites could result to getting fired because it breaches the Codes of Practise. As a HS Smith employee it would be best to avoid that. Also sending out harassing emails to others could issue you a warning. In order for the codes of Practise to be handled, inappropriate websites should be blocked and employees should only be able to send a certain amount of emails. If the codes of practise have been broken, a warning would be issued and the person would have limited internet use and limited emails that they can be able to send.