Current Relevant IT legislation, IT Implications and Applications

Unit R012 - Understanding tools, techniques, methods and processes for technological solutions

Introduction

- Most of the UK IT legislation relates to the protection of the individuals, organisations, technical equipment, information and intellectual property.

- Main IT legislation to be aware of:
  - Data Protection Act (1998)
  - Copyright, Designs and Patents Act (1988)
  - Computer Misuse Act (1990)
  - Health and Safety at Work Act (1974)
  - Freedom of Information Act (2000)

Data Protection Act (DPA) 1998

- The **DPA** aims to **protect** the **rights** of the **owner** of data
- It **does** not **protect** the **data itself**.
- The **act** sets out **rules** on how the **data** should be **stored** and **processed**.
- If the owners of the data think their data is being **misused** then the **DPA** can be **used** to **complain** and claim compensation.
- The **DPA** tries to **protect individuals** by giving them **rights** to **access** any **data** about **themselves** stored by others.

Data Protection Act (DPA) 1998

- The **DPA** gives everyone the **right** to know what **data** is stored about **them** on a **business computer** system and the right to see it.

- If someone feels that they are **not** being **allowed** to see the **data**, they can **contact** the **government** who will investigate and take action if needed.

- The DPA has **8 principles** about how personal data should be handled by anyone storing the data.

Data Protection Act (DPA) 1998

1. **Personal data must be fairly and lawfully processed.**
   - This means that personal data must not be collected by misleading the person into providing it and the data collected can only be used lawfully.

2. **Personal data must be processed for limited purposes.**
   - This means that personal data must only be used for the purpose for which it was obtained.

3. **Personal data must be adequate, relevant and not excessive.**
   - This means that personal data that is stored should be just enough for the task to be carried out, only relevant for the task, and not include other data.

Data Protection Act (DPA) 1998

4. **Personal data must be up to date**
   - This means that the person storing the data has a duty to ensure that any data they hold is accurate and free from errors.

5. **Personal data must not be kept for longer than necessary**
   - This means that data should be destroyed or deleted when it is no longer needed. This should be carried out to ensure that others cannot read or access it.

6. **Personal data must be processed in line with the individuals rights**
   - This principle ensures that the persons data is processed so that their rights are respected.

Data Protection Act (DPA) 1998

7. Personal data must be kept secure

- Any stored data must be secure. The DPA ensures that businesses that hold data must take precautions against its loss, unauthorised access and damage.

8. Personal data must not be transferred to other countries outside the European Economic Area that do not have adequate data protection.

- Other countries around the world may not have the same level of data protection as the UK, so the act states that personal data must not be sent to countries with lower levels of data protection than those in the UK.

GDPR – A New Regulation

- A new DPA - Enforcement date: 25 May 2018
- It brings into **align** data **privacy** laws across **Europe**
- After that **non-complying** organisations could face **heavy fines**
- Affects outside the EU as well if they sell goods or services to the EU.
- Applies to all companies holding personal data of EU citizens

Copyright, Design and Patents Act 1988

- This act makes it **illegal** to **copy** a work **without** the **permission** of the owner or copyright holder.
- It is also **illegal** to make **unauthorised copies** of **software**.
- People and business that **break** this **law** risk having to pay a **large fine**.
- Copyright law lasts for many years after the initial publication of work but only gives **limited protection** to the **person** who has created it.
- A problem of this act is that it is **difficult** to **trace** who has copied a piece of work, especially with computer software, images and other digital data.

Copyright, Design and Patents Act 1988

- Three common ways in which the law is most commonly broken:

1. Using software without correct software licence

- e.g. a licence is valid for 3 work PCs and the business installs it on more

2. Downloading files from the internet

- Permission to use text, images and other files must be obtained. The name of the copyright holder should be acknowledged too.

3. Copying music, DVDs, CDs and software

- Any copying or sharing of digital files that you have not created yourself is a breach of copyright, e.g. you can not share mp3 files from a CD you have burned.

Computer Misuse Act 1990

- This act aims to **protect data** and information that is held on **computer** systems.
- The **CMA** relates to **illegal access** to **files** and data **stored** on **computer** systems.
- It was introduced to cope with the **increase** in **hacking** and viruses.
- **Penalties** for breaking this law can be a prison sentence, fine, or both.
- There are three main parts:

Computer Misuse Act 1990

1. **Unauthorised access to computer material**

   Otherwise known as "hacking".

2. **Unauthorised access with intent to commit or facilitate the commission of further offences**

   Accessing computer material with the intent of using the material to commit further offences is against the law.

3. **Unauthorised acts with intent to impair operation of a computer**

   This means that any unauthorised alterations made to computer materials is against the law. Examples of how this law is broken is by sending viruses that impair operation.

Health and Safety at Work Act 1974

- To make **employers look after** the **Health** and **Safety** of **employees** and of the **public**.
- This act provides **guidance** to employers and employees when **working** with **computer** systems.
- The act also defines **actions** that an **employer** should **take** to **protect employees** who work with computers in their job.
- **Almost everyone** – not just all employees and employers – has a duty under the H&S act to **work** and **behave safely**.
- The act also makes it **illegal** to act **recklessly** or **intentionally** to act in such a way as to **endanger yourself** or **others**.
- Employees must take **reasonable care** for their own and others' safety and must cooperate with their employers in doing so.

Health and Safety at Work Act 1974

- The main law covering the use of computer equipment is the Health and Safety (Display Screen Equipment) Regulations. These state that employers must do five main tasks to ensure the safety of their employees.

1. Analyse workstations and assess and reduce risks

Employers need to check that the computer equipment and area around it is safe.

2. Ensure all workstations meet the minimum requirements

Employers need to make sure that adjustable chairs and suitable lighting are provided for employees, monitors can tilt and swivel, there is sufficient space for keyboards, monitor and any paperwork.

Health and Safety at Work Act 1974

3. Plan work so that there are breaks or changes of activity

Regular breaks should be provided or change in the activity that the employees are carrying out.

4. Arrange and pay for eye tests and glasses (if special ones are needed)

Employees of a business, who are covered by these regulations, can ask that eye tests are arranged and paid for. The business will only have to pay for glasses if special ones are needed.

5. Provide health and safety training and information

Employers must provide training to make sure that employees can use their computer equipment correctly. Employers should also provide information to their employees about health and safety when using screen equipment and how to minimise risks.

Freedom of Information Act 2000

- This act provides **public access** to **information** help by **public authorities**. It does it in two ways:

1. Public authorities are **obliged** to **publish certain information** about their activities.

2. Members of the **public** are entitled to **request information** from public authorities.

Freedom of Information Act 2000

- The act **covers** any **recorded information held** by a **public authority**.
- **Recorded information** includes any **information** that is held on **printed documents**, **computer-based files**, letters, emails, photographs and sound/video recordings.
- The act **does not give** people **access** to their **own** personal **data**, such as credit reference files or health records.
- If someone wants to **see** their **own data** then they should make a **subject access** request under the **DPA**.
- **Anyone** can make an FoI **request** to a public **authority** and it is the **responsibility** of the **public authority** to **respond**.

Ethical and Moral Issues

- With the increased use of computer systems to hold and share data and information, there are some ethical and moral issues that should always be considered.
- Care should be taken to make sure that **information** and **equipment** is **not misused**.
- Another consideration when using the internet, for example, social media, is to avoid **defamation** of **character**.
- It is very easy to **post comments** that are **not true.**
- **Defamation** of **character** is when an **untrue** or **false statement** is made by **one person about another**.

Ethical and Moral Issues

- This can also be known as trolling or **cyber-bullying** and can be done by **posting untruths/cynical comments**.
- Some trolls specialise in posting untrue/false comments about celebrities.
- Another consideration is that of libel. **Libel** is a written comment that is **damaging** to a **person's reputation**.
- A good rule of thumb is that if you wouldn't say it to someone's face, don't post it online.