Level 1/2 Vocational

ICT

1.3.5 How legal issues protect computer users

General Data Protection Regulation (GDPR) 2018

The GDPR was introduced to standardise data privacy laws across the EU, protecting individuals' rights by controlling how organisations handle personal data. This includes personal details, online identifiers, location data and genetic information.

Organisations must:

- process personal data securely
- implement security measures from the start
- maintain security effectively throughout the system's life.

The GDPR gives individuals more control over their personal data and places clear obligations on organisations that process it.

Data Protection Act (DPA) 1998

With the rise of computer systems, the DPA 1998 was created to protect personal data. It sets rules for how organisations collect, process and store personal information. Individuals have the right to access their own data through subject access requests.

The DPA is based on eight key principles:

1. **Fair and lawful:** Data must be collected and used fairly and legally.
2. **Purpose:** Data must be held and used only for specific, registered reasons.
3. **Rights:** Data can only be used for registered purposes and disclosed to named individuals.
4. **Adequacy:** Data kept must be relevant and not excessive.
5. **Accuracy:** Data must be accurate and kept up to date.
6. **Retention:** Data should not be kept longer than necessary and must be safely destroyed afterwards.
7. **Security:** Data must be kept safe and secure.
8. **International transfers:** Data should not be transferred outside the European Economic Area unless the receiving country has adequate data protection.

Computer Misuse Act 1990

This Act protects against computer crime, including:

- **Unauthorised access:** Hacking into computer systems
- **Unauthorised access and modification:** Planting malware or spyware, electronic vandalism or theft of information

The Act covers unauthorised access with the intent to commit a crime and also makes it illegal to create, supply or obtain anything used for computer misuse offences.

Communications Act 2003

This Act regulates telecommunications in the UK, covering television, telephone calls and the internet. It established Ofcom as the industry regulator, responsible for promoting media literacy.

It makes it an offence to:

- send malicious messages via social media
- use internet services without intending to pay.

Regulation of Investigatory Powers Act (RIPA) 2016

RIPA 2016 provides a legal framework for law enforcement and security agencies to use investigatory powers. This includes:

- surveillance of communications (for example bugs and video)
- interception of private communications (for example emails and phone calls).

It applies to both private and public networks and services, covering all types of communication, including the Internet of Things (IoT).

Copyright, Designs and Patents Act 1988

This Act gives the creator of a work the sole right to copy, adapt, communicate, lend or sell copies of their work. This right can be transferred. It covers literary, dramatic, musical and artistic works, allowing creators to control how their material is used. It also protects against music and movie piracy.

Health and safety legislation

This includes two key acts:

Health and Safety at Work etc Act 1974

- Ensures a safe working environment for all employees.
- Requires regular checks of computer and electrical equipment.
- Employers must have safety policies, and employees must report hazards (f.e. trailing wires).

Health and Safety (Display Screen Equipment) Regulations 1992

- Focuses on the safe use of computer monitors and equipment.
- Employers must ensure employees understand safe computer use.
- Promotes correct posture: appropriate chair, correct screen height and distance to prevent headaches or eye strain.