# **Topic 4: Legal, Moral And Ethical Issues**

## 18 Computer Law And Ethical, Moral And Social Issues

### Legal Issues

**Copyright, Designs and Patents Act 1988**

PURPOSE:

- Original work remains the intellectual property of the author.

- Material is protected from being copied without the author’s permission.

- People are paid for their original work and there is a legal process to follow if the work is copied or stolen.

SOFTWARE INFRINGEMENTS INCLUDE:

- Pirating copyrighted software.

- Using copied software.

- Transmitting pirated software on websites.

- Installing too many copies of software onto a network.

- Lending or renting copyrighted software without the owner’s permission.

- Making changes to copyrighted material without the author’s permission.

IMPLICATIONS:

- Detecting breaches is difficult.

- Prosecution is rare.

- Organisations need to keep careful records of what software is installed and whether they have the correct licenses.

- Software is expensive so it encourages people to pirate.

- Many people don’t see piracy of software as “stealing”.

- Its easy to break these laws.

**Computer Misuse Act 1990**

PURPOSE:

- Legislate against hacking, malware and computer crime.

-Set out penalties for different levels of unauthorised access.

RECOGNISED OFFENCES:

- Unauthorised access to computer material.

- Unauthorised access to computer material with the intent to commit or facilitate a crime.

- Unauthorised modification of computer material.

- Making, supplying or obtaining anything that can be used in computer misuse offences.

IMPLICATIONS:

- Proving intent is difficult - people plead ignorance.

- Tracing who is responsible for computer misuse is often difficult.

- Organisations will often not press charges as they do not want the bad publicity that comes with being hacked.

**Data Protection Act 1998**

PURPOSE:

- Protect individuals from the misuse of information stored about them by organisations.

- Sets out responsibilities for organisations who hold data.

WHY IS IT NEEDED?:

- There is a huge amount of information about us held by a wide variety of organisations.

- Data held on a computer is at a higher risk from misuse than paper-based records.

RISKS TO DATA SECURITY:

- Portability: easy to copy large amounts of data to small devices.

- Editing: someone can change computer records without being easily detected.

- Points of access: Potential to access data from any computer on a network.

DEFINITIONS:

- Personal Data: data relates to a living, identifiable individual.

- Data: both computer and paper-based information that forms part of a record about an individual.

- Data Subject: the individual whom the data is stored about.

- Data Controller: the person responsible for implementing the provisions of the Data Protection Act within an organisation.

DATA PROTECTION ACT PRINCIPLES:

Make Sure Information Is:  
**FL** - Used Fairly and Lawfully.

**L** - Used for limited, specifically stated purposes.

**ARE** - Used in a way that is adequate, relevant and not excessive.

**A** - Accurate.

**AN** - Kept for no longer than is absolutely necessary.

**PR** - Handled according to people’s data protection rights.

**SS** - Kept safe and secure.

**EU** - Not transferred outside the European Economic Area without adequate protection.

This gives the easy acronym **FL-ARE-L-AN-A-PR-EU-SS**

**Regulation Of Investigatory Powers Act 2000**

PURPOSE:

- Allow suitable authorities (police, security services) access to communications to:

- Prevent or detect crimes.

- Prevent public disorder.

- To ensure the national security and safety of the general public.

- To investigate or detect any abnormal or illegal use of telecommunication systems.

It is illegal for anyone who is not authorised under the act to carry out surveillance and monitoring of communications.

UNDER THIS ACT POLICE AND OTHER GOVERNMENT DEPARTMENTS HAVE THE RIGHT TO:

- Demand ISPs provide access to the customer’s communications.

- Allow mass surveillance of communications.

- Demand ISPs fit equipment to facilitate surveillance.

- Demand access be granted to protected information.

- Allow monitoring of an individual’s internet activities.

- Prevent the existence of such interception activities being revealed in court.