

---

# A-level Computing

## List of current legislation relevant to the specification

---

Legislation is listed in chronological order. New legislation will be added as relevant.

### **Health and Safety (Display Screen Equipment) Regulations 1992**

These regulations relate to the Health and Safety of individuals using computers in a work context. Employers, employees and manufacturers all have certain responsibilities.

Employers must

- evaluate the health and safety conditions workstations give rise
- train employees in the safe use of equipment
- ensure employees take regular breaks or changes in activity
- provide regular eye tests and pay for glasses

Employees must

- use workstations correctly according to their training
- bring problems to the attention of their employer and co-operate in their correction

Manufacturers must ensure that

- screens have clear characters, are flicker free, swivel and tilt and are at an appropriate height
- that keyboards are separate from screen and tilt-able, have a matt surface to avoid glare, and have key symbols that are of adequate contrast and visibility.

### **Copyright, Design and Patents Act 1988**

Under this act it is illegal to:

- copy software or distribute software
- execute or run software for which you do not have a licence
- alter or edit software
- transmit software or send via a telecommunications link

This Act has been updated more recently by the Copyright and Related Rights Regulations 2003 which includes a section on Electronic Rights Management.

### **Computer Misuse Act 1990**

There are three levels of offence under this act:

- unauthorised access to computer material
- unauthorised access to computer material with criminal intent
- unauthorised modification of computer material

This law is also known as the “anti-hacking” act.

---

## **Data Protection Act 1998** (followed and updated the Data Protection Act 1984)

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Under the act, personal data is data kept about a living, identifiable individual person. Somebody who is the subject of personal data is called a data subject. Somebody who determines why and how personal data are processed is called a data controller.

There are a number of exemptions to the Act including: Personal, family and household use of your information; Safeguarding national security; The prevention and detection of crime and the apprehension or prosecution of offenders and examination scripts and marks.

## **Regulation of Investigatory Powers Act 2000**

Under the RIP Act it is an offence to intercept a message sent via public or private telecommunication system, although there are exemptions.

The Act regulates the power of government security services and law enforcement authorities by allowing the interception, surveillance and investigation of electronic data in specified situations such as when preventing and detecting crime.

Powers include being able to demand the disclosure of data encryption keys.