

The law and ethics

Computer-related laws exist to protect users. By being aware of the laws we can stay safe whilst online.

Computers and the law

Computers are fantastic - they help us to learn, share, communicate and find entertainment. However, it is also possible for computers to be used to aid illegal activities. An understanding of computer-related laws in the United Kingdom is needed to make sure we stay on the right side of the law.

Computers might be used unlawfully in many ways, for example:

- allowing someone to illegally share your personal data
- helping to steal financial information, such as credit card numbers or bank account details
- helping to illegally copy and distribute films, television programmes and music
- extorting information or blackmailing someone

Additionally, the internet allows people to commit crimes remotely, for example a hacker could gain access to a computer on the other side of the world. Laws are required to help deter such activities.



There are three laws to consider:

- Computer Misuse Act
- Copyright, Designs and Patents Act
- Data Protection Act

Computer Misuse Act

The **Computer Misuse Act** attempts to discourage people from using computers for illegal purposes. There are three separate parts to the Act:

1. It is illegal to access data stored on a computer unless you have permission to do so. Unauthorised access is often referred to as hacking.
2. It is illegal to access data on a computer when that material will be used to commit further illegal activity, such as fraud or blackmail.
3. It is illegal to make changes to any data stored on a computer when you do not have permission to do so. If you access and change the contents of someone's files without their permission, you are breaking the law. This includes installing a virus or other malware which damages or changes the way the computer works.

The maximum punishment for breaking this law is a £5000 fine or several years' imprisonment.

However, one key part of the law is that **intent must be proved**. If a computer is not well protected, someone could accidentally access its data without meaning to. Someone might also accidentally change a document without realising it. For anyone to be found guilty, it has to be shown that they intentionally accessed and changed data.

In order to make a successful prosecution under the Computer Misuse Act, the prosecutor must be able to prove intent.

Copyright, Designs and Patents Act

The **Copyright, Designs and Patents Act** exists to protect our creations.

When anyone creates something, they own it. What they create might include:

- a picture, drawing or photograph
- a video, television programme or film
- text, such as a book, article or report
- a game

Copyright is a legal means of ensuring that content creators can protect what they create. **Copyright is applied automatically - it is not necessary to register copyright or to use a © symbol.** Work is automatically protected by copyright unless the copyright holder chooses to give that right away.

Copyright gives the copyright holder exclusive rights to publish, copy, distribute and sell their creation. No one else can use the work without permission. Copyright on a piece of work lasts for a long time, although the rules about how long are quite complicated and vary from country to country.

When you buy something, such as a book, film or music CD, the copyright holder grants permission for you to use it as part of the sale. This is called a **licence**. The licence is generally only for you to use.

When using computers, unless you have permission with regard to a particular copyrighted material, it is illegal to:

- make copies
- publish
- distribute
- sell copies

This applies to any copyrighted material, such as music, films, games and television programmes. The internet has made it extremely easy to access copyrighted material illegally. **If you download a music track, film, game or programme without the copyright holder's permission, you are breaking the law.**

Supermarkets earn their money by selling food and other products. If someone takes their products without paying, the supermarket doesn't make any money. In the same way, musicians, photographers, film makers and artists earn their money by selling products. **If someone takes their products without paying, the person who created the work doesn't make any money.**



There are some situations where it is legal to copy, publish, distribute or sell material. These are:

- when you are the copyright holder
- when you have the copyright holder's permission
- when the copyright holder has chosen to give up their copyright

Data Protection Act

It is increasingly common for **personal details** to be stored on computers. The **Data Protection Act** exists to protect such details. This personal data includes items such as:

- name and address
- date of birth
- medical records
- school and employment records
- religion

Personal data is private and should only be accessible by authorised people. Also, digital files stored on computers can be easy to access, copy and share. Protection is needed to make sure that our personal data is kept private and not altered or deleted. **The Data Protection Act exists to ensure our data is properly looked after.**

In addition, **everyone has the right to see what data is held about them by an organisation, and to have that data corrected or deleted if incorrect.**

The Data Protection Act is built around eight principles which state how personal data should be treated:

1. **Personal data must be fairly and lawfully processed.** This means that an organisation must be truthful about what personal data they wish to collect and what they want to use it for.
2. **Personal data must be obtained for specified and lawful purposes.** This means that an organisation cannot use personal data for any purpose other than that stated when they collected the data. For example, if a company wanted your exam records to see if you were qualified for a job, it could not use those records to try and sell you revision guides that it thinks you might need. Also, the company cannot pass on your data to any other organisation without your permission.
3. **Personal data must be adequate, relevant and not excessive.** This means that an organisation cannot ask for any data that is not immediately needed. For example, when applying for a bank account, the bank cannot ask you where you went on holiday last year.
4. **Personal data must be accurate and up to date.** If data held about you is wrong or out of date, you have the right to have it corrected or deleted. This is extremely important, as incorrect or out of date data might, for example, prevent you from getting a job, a loan or from being able to buy a house.
5. **Personal data must not be kept for longer than is necessary.** As soon as an organisation no longer needs your data, they must delete it.
6. **Personal data must be processed in line with our rights.** Your rights include the right to see any data held on you, and the right to correct inaccurate data.
7. **Personal data must be held securely.** This means safe from unauthorised access (eg with usernames and passwords), but also safe from accidental loss (by making back ups).

8. **Personal data must not be transferred to other countries outside the European Economic Area, unless those countries have similar data protection laws.**

An organisation can face a large fine if they are found to be in breach of the Data Protection Act.