

# ICT Legislation Booklet



# The Copyright Designs and Patent Act 1988

A Copyright work could be marked with ©, the owner's name, and the year it was created but this is not necessary as copyright is an automatic right

## About copyright

You should only copy or use a work protected by copyright with the copyright owner's permission.

Copyright **applies to any medium**. This means that you must not reproduce copyright protected work in another medium without permission. This includes, publishing photographs on the internet, making a sound recording of a book, a painting of a photograph and so on.

**Copyright does not protect ideas for a work.** It is only when the work itself is fixed, for example in writing, that copyright **automatically** protects it. This means that you do not have to apply for copyright. If you can record the idea on paper then it can be protected by copyright.

A copyright protected work can have more than one copyright connected to it. For example, an album of music can have separate copyrights for individual songs, sound recordings, artwork, and so on. Whilst copyright can protect the artwork of your logo, you could also register the logo as a trade mark.

## Ownership of copyright works

### Creator and first owner

The creator of an original copyright work is usually the first owner.

### Works created for an employer

The same rule does not apply for works created by an employee in the course of his employment. Normally your employer will own the copyright on works created as part of your job.

## Copyright protects:

**literary works**, including novels, instruction manuals, computer programs, song lyrics, newspaper articles and some types of database, websites and the internet

**dramatic works**, including dance or mime

**musical works**

**artistic works**, including paintings, engravings, photographs, sculptures, collages, architecture, technical drawings, diagrams, maps and logos

**layouts or typographical arrangements** used to publish a work, for a book for instance

**recordings** of a work, including sound and film

**broadcasts** of a work

### **Commissioned works**

A commissioned work is when you pay someone else to do something for you. If you hire a Wedding Photographer they will own the copyright on the photographs unless they agree to sign an agreement that says otherwise.

### **Joint authors**

A single work may be created and owned by more than one person. For example two people may work on a book together. Both would own the copyright

### **Other people's copyright works**

If you want to use, change, adapt, broadcast or copy someone else's copyright works you need to seek permission from the owner.

The owner may let you buy the copyright or, obtaining a licence for your agreed use. Locating the copyright owner can sometimes be difficult but failure to get permission may result in legal action against you.

<b>How long does copyright last?</b>	
Literary (written)	life of the creator plus 70 years from the end of the year in which they died
theatrical (dramatic)	life of the creator plus 70 years from the end of the year in which they died
musical or artistic	life of the creator plus 70 years from the end of the year in which they died
Sound Recordings	life of the creator plus 50 years from the end of the year in which they died
Broadcast (TV show)	life of the creator plus 50 years from the end of the year in which they died
Published editions	life of the creator plus 25 years from the end of the year in which they died

People break copyright law on a daily basis without realising it.

- by downloading films, music, programs from the internet without paying for them
- making copies of CDs and DVDs for their friends – or even worse to sell
- photocopying large sections from books

# FREE MUSIC MYTHS

## FACT:

Writing, recording and releasing is a business, one that requires constant investment in order to bring new artists to the public and develop artist careers over the long term. Without this investment, many budding artists are unlikely to ever get heard. The fact is illegal file-sharing is cutting into legitimate sales. The impact has been immense. Live touring has always been a source of income, but it cannot fund an entire career nor can it sustain many non-performance based genres. The expenses of going on the road mean that profits, while healthy in some cases, are in the majority of cases offset by the costs. Even when a new artist is discovered over the internet, and has stood out from the crowd, unless enough people buy the track, either via a legitimate site or in a physical format (CD or DVD), they won't be able to make a living. A few artists of course do become big stars and with it they gain high financial rewards. But for the industry that has invested in them, the profits are ploughed back into funding new artists.



**If consumers want a wide choice and variety of music, if they want their favourite artists to succeed or to continue to discover new talent, the best way is to buy their music and go to and see them perform.**

---

## Some of the most commonly repeated myths about the recording industry and music online

**"These artists are very rich anyway, downloading a few tracks for free isn't hurt them."**



The overwhelming majority of artists are NOT rich. The biggest losers are the upcoming artists because not paying for music means much less money to invest in them.

**" 'Free music' sounds great. What's the problem?"**



The problem is that the artists, and the hundreds of others who helped create the recording will not get paid for their efforts. The music is generally taken without permission, and often before its ready to be released in the way the artists determine.

**"Piracy on the Internet may be a problem, but nothing can be done to stop it."**



The recording industry has already taken action against thousands of sites around the world and a large number of individuals that illegally distributed files on P2P networks. The vast majority of sites take down illegal material when asked to do so. If they don't there is the final option of legal action. Educational programmes, support for legal websites, and a call to ISPs to install technological 'blocks' are also part of the industry's response to the problem.

**"Uploading music without the consent of the creator may be illegal, but isn't the music industry exaggerating the effect on the music sector?"**

There is overwhelming evidence that unauthorised copying and distribution means less music is sold. Extensive extensive studies have show a "close linkage between changes in file-sharing and changes in record sales", bringing "significant harm to the music industry"

[www.journals.uchicago.edu/jle/journal](http://www.journals.uchicago.edu/jle/journal)

**"The real problem is that the music industry wants to stop the advance of technology."**

The music industry wants the advances technology brings, but does not want that technology abused at the expense of a whole industry. From the Edison cylinder, through vinyl, tape and the CD, to the MP3 file, the music industry has embraced new forms and new ideas and is doing so more than ever before and faster than other 'content' industries.

**"There are no legitimate services out there for me to use, so I'm forced to fall back on the illegitimate ones."**

There are already many legitimate services (like I-Tunes) offering millions of tracks - and more are appearing all the time.

The price of a CD or a track has fallen or remained static in most countries, but piracy has got worse. When you pay for a CD or MP3, you're paying for the costs involved in developing, making, marketing and distributing music. The people who pay these costs cannot compete with music given away for 'free'.

**"I've heard artists claim that making their music available to download for free is the best way to get themselves heard, in that way promoting their music and boosting their sales."**

Many artists do in fact choose to make their music available for promotion. Generally this will be accompanied by a marketing push for a future single or album and will be a means of raising a profile for future sales. But, importantly, this is the artists' and other rights holders' choice and has been done for a good reason. It is not up to someone else to decide what gets distributed for free.

**"None of the money from online sales goes to the artist anyway."**

Record companies pay artists royalties on sales of downloads in the same way as for sales of CDs.

**"File sharing and burning is just like home taping, and that never killed the music sector."**

File sharing on the internet is nothing like copying tapes at home. That's like comparing someone physically copying a letter to a printing house churning out hundreds of copies a minute of the same letter - and then making it available to an unlimited number of people around the world for free.

# Computer Misuse Act 1990 – (CMA 1990)

The Computer Misuse Act was introduced to tackle a sudden rise in computer related crime that the existing Laws were not able to cope with.

The Act has three main parts, each part describe a new offence created by the Act.

## 1. Unauthorised access to computer material

This makes it illegal to access a computing system unless authorised to do so.

NOTE: This includes logging onto the school network as another pupil. The school only gives YOU permission to use YOUR OWN log on.

This part of the Act makes computer hacking illegal

## 2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence

This covers the situation where unauthorised access is gained with intent to commit a further offence. For example, a person may gain unauthorised access to a computer via another person's User ID or logon in order to transmit offensive material.



This part of the Act makes computer fraud and blackmail illegal

## 3. Unauthorised modification of computer material

This offence includes the deliberate deletion or corruption of programs or data. It also includes the introduction of viruses etc., where these result in the modification or destruction of data.



This part of the Act makes it illegal to knowingly send someone a computer virus

The first of these three offences would most likely be dealt with in a Magistrates Court, but the second two are considered to be serious and would be referred to the Crown Court where very large fines and/or gaol sentences are possible.

Further Information:

[http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm)

# Data Protection Act 1998

The Data Protection Act helps to control the data that is collected, stored and processed about people by organisations like companies and schools.

**Data subjects** are people like you and me. A data subject can be an individual or a group of individuals.

**The data controller** is the person within an organisation who is responsible for the data it holds and processes.

**The Information Commissioner (ICO)** is responsible for the promotion and enforcement of the DPA.

## How does this affect me?

- Organisations can only use the data they collect for the purpose they collected it for.
- As a data subject you have the right to request access to the information an organisation hold about you for a fee of up to £10.

For example if a company has your details because you buy energy from them, it would be illegal for them to use this information to send you information about a new credit card they are launching because that is not why they collected the information, and as a customer you would not expect it to be used in that way.

## Further information:

<http://www.ico.gov.uk/>

[http://www.ico.gov.uk/what\\_we\\_cover/data\\_protection.aspx](http://www.ico.gov.uk/what_we_cover/data_protection.aspx)

[http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG\\_10031451](http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG_10031451)

## Exemptions from the Act

Not all data is covered by the Act, can you think why?

- Tax records
- Crime records
- National Security
- Domestic use (your own personal address book)
- Data that does not identify the person it belongs to

## In the DPA data is Information that:

- Is being processed automatically by equipment
- Is recorded to be processed
- Is part of a relevant filing system
- Forms a record of the health or education of an individual

## A relevant filing system

A paper based system (usually), where the information is structured in such a way that it can be readily accessed.

For example:

Alphabetical, numerical, date order

# Freedom of Information Act 2000 (FOI 2000)

The Freedom of Information Act gives individuals or organisations the right to request information from any public authority, for Example you could use the FOI to request information from Wigan Council,

The Act gives you the right to request information held by public authorities, companies wholly owned by public authorities in England, Wales and Northern Ireland and non-devolved public bodies in Scotland.

## Key Facts

- Applies to Public Authorities like the BBC, Environment Agency, Wigan Council etc.
- Affects everyone in the organisation and therefore staff must be aware that anything they record could be seen by someone outside the organisation
- Allows anyone, no matter who they are or where they live to make a request for information.
- Works in conjunction with the Data Protection Act.
- 20 working days to respond to request.
- Specifies exemptions covering information that does not have to be released.
- Is regulated by the Information Commissioners Office.

### Information Exempt from disclosure under FOI

- Information accessible by other means
- Court records
- Parliamentary privilege
- Personal information (available under Data Protection Act)
- Information provided in confidence
- Information prohibited by or under any enactment; Information incompatible with any community obligation; Information which could be in contempt of court

## Examples

People researching their family history used the FOI to obtain records about their ancestors from the 1911 census (a record of everyone in England in 1911) before it was due to be released in 2011.

Newspapers often use the FOI to obtain information they can use to support a story they are writing, often about how the Government has been spending tax payers money.

### Information that is only supplied when it is in the public interest

- Information intended for future publication
- Investigations & proceedings conducted by public authorities
- Law enforcement
- Health & safety
- Environmental information (available under [Environmental Information Regulations](#))
- Legal professional privilege
- Commercial interests

## Further information:

[http://www.bbc.co.uk/foi/about/foi\\_explained.shtml](http://www.bbc.co.uk/foi/about/foi_explained.shtml)

[http://www.opsi.gov.uk/acts/acts2000/ukpga\\_20000036\\_en\\_1](http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1)

# Health & Safety at Work Act 1974

All workers have a right to work in places where risks to their health and safety are properly controlled. Health and safety is about stopping you getting hurt at work or ill through work. Your employer is responsible for health and safety, but **you** must help.

## Health & Safety at Work

### What employers must do for you

1. Decide what could harm you in your job and take precautions to stop it.
2. In a way you can understand, explain how risks will be controlled and tell you who is responsible for this.
3. Consult and work with you and your health and safety representatives in protecting everyone from harm in the workplace.
4. Free of charge, give you the health and safety training you need to do your job.
5. Free of charge, provide you with any equipment and protective clothing you need, and ensure it is properly looked after.
6. Provide toilets, washing facilities and drinking water.
7. Provide adequate first-aid facilities.
8. Report injuries, diseases and dangerous incidents at work to the HSE
9. Have insurance that covers you in case you get hurt at work or ill through work.
10. Display a hard copy or electronic copy of the current insurance certificate where you can easily read it.
11. Work with any other employers or contractors sharing the workplace or providing employees (such as agency workers), so that everyone's health and safety is protected.

### What you must do

1. Follow the training you have received when using any work items your employer has given you.
2. Take reasonable care **of your own** and other people's health and safety.
3. Co-operate with your employer on health and safety.
4. Tell someone (your employer, supervisor, or health and safety representative) if you think the work or inadequate precautions are putting anyone's health and safety at serious risk.

Further information:

[www.hse.gov.uk/pubns/law.pdf](http://www.hse.gov.uk/pubns/law.pdf).

[www.http://www.hse.gov.uk/legislation/hswa.htm](http://www.hse.gov.uk/legislation/hswa.htm)

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



## Who is affected?

The Regulations apply where staff habitually use VDUs as a significant part of their normal work. People, who only use VDUs occasionally, are not covered by the requirements in the Regulations (apart from the workstation requirements).

**Note:** These regulations do not apply to students in schools or colleges.

## Are aches and pains caused by using a VDU? What about 'RSI'?

Some users may get aches and pains in their hands, wrists, arms, neck, shoulders or back, especially after long periods of uninterrupted VDU work.

Repetitive strain injury (RSI) has become a popular term for these aches, pains and disorders, a better medical name for this whole group of conditions is 'upper limb disorders'. Usually these disorders do not last, but in a few cases they may become persistent or even disabling.

## How can I avoid these aches, pains and disorders?

Problems of this kind may have a physical cause, but may also be more likely if a VDU user feels stressed by the work. If you get aches or pains you should alert your supervisor or line manager.

## What an Employer must do

Employers have to analyse workstations, and assess and reduce risks by looking at:

- the whole workstation including equipment, furniture, and the work environment;
- the job being done; and
- any special needs of individual staff.

Employees and safety representatives should be encouraged to take part in risk assessments, eg by reporting health problems. Where risks are identified, the employer must take steps to reduce them.

## Ensure workstations meet minimum requirements

Workstations should have adjustable chairs, suitable lighting and enough space for the screen, keyboard and mouse etc on the desk. The general work environment and software used must also meet requirements.

## Plan work so there are breaks or changes of activity

As the need for breaks depends on the nature of the work, the Regulations require breaks or changes of activity but do not specify their timing or length. However in general short, frequent breaks are better than longer, less frequent ones. Ideally the individual should have some discretion over when to take breaks.

## Eye Tests

Employees covered by the Regulations can ask their employer to provide and pay for an eye and eyesight test. There is also an entitlement to further tests at regular intervals. Employers only have to pay for spectacles if special ones (for example, prescribed for the distance at which the screen is viewed) are needed and normal ones cannot be used.



### **Provide health and safety training and information**

Employers must provide training, to make sure employees can use their VDU and workstation safely, and know how to make best use of it to avoid health problems, for example by adjusting the chair.

### **What can I do to help myself?**

Take notice of any training you are given and make full use of the equipment provided, and adjust it to suit you and avoid potential health problems.

## **Getting comfortable**

### **Keying in (Typing)**

- Adjust your keyboard to get a good keying position. A space in front of the keyboard is sometimes helpful for resting the hands and wrists when not keying.
- Try to keep your wrists straight when keying. Keep a soft touch on the keys and don't overstretch your fingers. Good keyboard technique is important.



### **Using a mouse**

- Position the mouse within easy reach, so it can be used with the wrist straight.
- Sit upright and close to the desk, so you don't have to work with your mouse arm stretched. Move the keyboard out of the way if it is not being used.
- Support your forearm on the desk, and don't grip the mouse too tightly.
- Rest your fingers lightly on the buttons and do not press them hard.



### **Reading the screen**

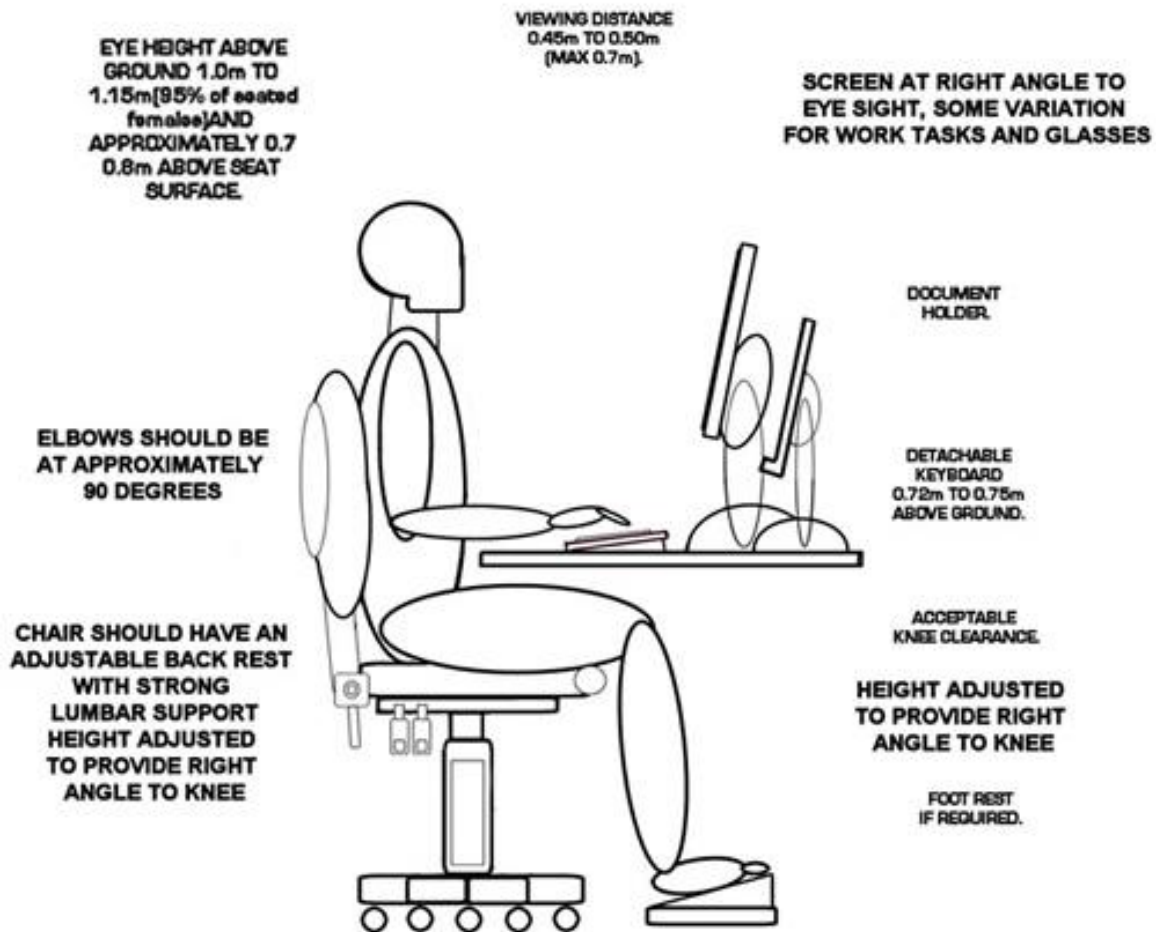
- Adjust the brightness and contrast controls on the screen to suit lighting conditions in the room.
- Set up software, so that text is large enough to read easily on your screen.
- Select colours that are easy on the eye (contrast).
- Individual characters on the screen should be sharply focused and should not flicker or move.
- Make sure the screen surface is clean.



### **Posture and breaks**

- Don't sit in the same position for long periods.
- Avoid repeated stretching to reach things you need (if this happens a lot, rearrange your workstation)
- Most jobs provide opportunities to take a break from the screen, eg to do filing or photocopying. Make use of them. Frequent short breaks are better than fewer long ones.

## A suitable work station



### Further information:

[www.hse.gov.uk/pubns/indg36.pdf](http://www.hse.gov.uk/pubns/indg36.pdf)

<http://www.nhs.uk/LiveWell/WorkplaceHealth/Pages/Howtositcorrectly.aspx>

[http://www.direct.gov.uk/en/Employment/HealthAndSafetyAtWork/DG\\_10026668](http://www.direct.gov.uk/en/Employment/HealthAndSafetyAtWork/DG_10026668)

# Regulation of Investigatory Powers Act 2000 (RIPA 2000)



In its efforts to detect crime over the Internet, the British government introduced the Regulation of Investigatory Powers (RIPA) Act in July 2000.

The RIPA gives a limited group of authorities working for the police, Customs, and secret services, the right to demand information about individuals' Internet and mobile phone habits from Internet Service Providers (ISPs) and mobile phone companies.

Under RIPA, ISPs linking computers with the Internet can be forced to install "black boxes" which would allow security forces to monitor e-mail messages.

The authorities could also force individuals and companies to decode encrypted messages or face prosecution.

Critics fear this gives security forces powers to invade the privacy of British citizens.

The British government has admitted that the new law might result in information being inadvertently collected about innocent citizens, but that this is necessary to track, trace and tap high-tech criminals.

## European Convention on Human Rights

RIPA was an important step forward to ensure investigatory techniques are used in a way that is compatible with our right to private and family life, enshrined in the European Convention on Human Rights.

## Who uses covert techniques?

Public authorities such as police and local authorities have for many years been able to use a range of covert techniques to investigate suspects without alerting them to the fact that they are under investigation.



RIPA makes sure these techniques are used in a regulated way. This means that any authorising officer must first consider whether the use of covert techniques is necessary and proportionate before agreeing that the techniques can be used.

## What does RIPA 2000 regulate?

- the interception of all communications, such as telephone calls, emails or letters
- *intrusive surveillance* which is carried out covertly either in private premises or vehicles
- *directed surveillance* which is carried out covertly in public places where private information likely to be obtained about a particular person
- the use of informants or undercover officers
- access to electronic data protected by encryption or passwords

## RIPA provides important safeguards

- RIPA strictly limits:
  - the public authorities which can use and authorise these techniques
  - the purposes for and conditions in which they can be used
  - the way the material obtained must be handled
- reserves the more intrusive techniques for intelligence and law enforcement agencies acting against only serious crime or threats to our national security
- sets out the role of independent commissioners who hold judicial office to oversee the use of covert techniques
- establishes an independent tribunal to hear complaints from those who believe the techniques have been used inappropriately.

## **Investigatory Powers Tribunal**

The tribunal, which was set up by RIPA and replaced the Interception of Communications Tribunal, is designed to deal with complaints from the public about surveillance by the intelligence services and the police.



The tribunal investigated over 102 complaints against the security services during 2001, but upheld none.

It was set up to sit in secret but, after a challenge by the Guardian newspaper under the Human Rights Act, will now sit in public when there is no "threat to national security".



## Internet Code of Practice (ICOP)

The internet is not owned by a single organisation or person therefore everyone who uses the internet is responsible for keeping it safe for everyone to use. Internet Service Providers (ISPs) like AOL, BT Broadband and Virgin Media are expected to follow the Internet Code of Practice.

The ICOP is constantly changing because the Internet is constantly changing.

The main aims of the Internet Code of Practice are:

- Children's sites should only contain material suitable for children
- Web pages that may offend some people should have a warning first
- Links to other sites should be checked to make sure they are not offensive
- People should not send SPAM email (unsolicited or junk email)
- Adverts on the internet should tell the truth
- Extra charges should be clearly shown (VAT, post and packaging)
- People must seek permission from the copyright owner or copyright material to use it on the internet where anyone can see it
- Private information about individuals should not be disclosed (made available)
- Large media files like images and music should be compressed to reduce download times
- Information on the web should not encourage people to break the law
- Information should not be deliberately misleading
- Website owners should check the files available on their website are virus free
- ISPs should make their subscribers aware of the code of practice and enforce it

### What you can do

- Always think before you post
- Avoid using swear words and bad language online – you never know who might read it
- Think carefully about the images, videos and sound files you upload – do you really want just anyone to be able to see/hear them?

### More information

<http://www.internet.org.uk/icop.html>