

## IT policies - relevant legislation

High level summaries of various points that might be relevant to users and system administrators as it pertains to the creation, processing, storage, and transmitting of information. These sections also provide the governance underpinning the MET's information and cyber security policies, standards, and other guidance.

### Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:

- unauthorised access to computer material
- unauthorised access with intent to commit or facilitate commission of further offences
- unauthorised modification of computer material

### The Data Protection Act

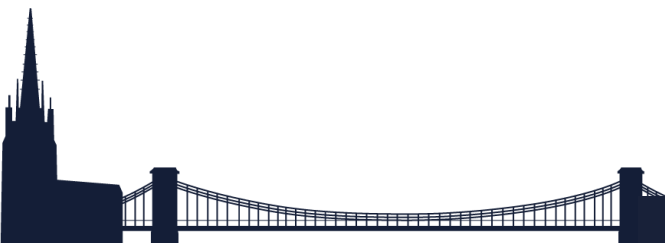
The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions



- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences..

### **The Privacy and Electronic Communications (EC Directive) Regulations 2003**

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

### **The Malicious Communications Act 1988**

The Malicious Communications Act 1988 (MCA) deals with the sending of offensive communications. It was written before the widespread use of the internet. However, in this day and age, it is frequently used to prosecute offences that are committed on social media.

The MCA makes it an offence to send any kind of written, verbal or electronic communication that conveys a message that:

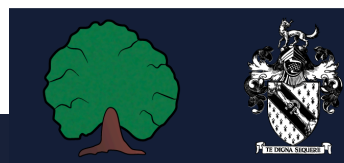
- is indecent or grossly offensive;
- makes a threat; or
- contains information that is false and known or believed to be false by the sender

### **Freedom of Information Act 2000**

The [Freedom of Information Act 2000](#) is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability.

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

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use



of communications data and can be invoked in the cases of national security, and for the purposes of detecting crime, preventing disorder, public safety and protecting public health.

### **Defamation Act 2013**

“Defamation is a false accusation of an offence or a malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation’s reputation from harm.”

### **Obscene Publications Act 1959 and 1964**

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

### **PREVENT Duty Guidance 2015 and 2023**

“The Prevent strategy, published by the UK Government in 2011, is part of [the UK’s] overall counter-terrorism strategy, CONTEST. The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. In the Act this has simply been expressed as “prevent people from being drawn into terrorism”. The Prevent strategy has three specific strategic objectives:

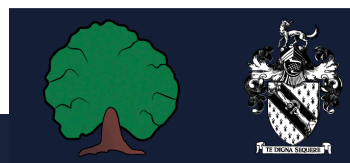
- Respond to the ideological challenge of terrorism and the threat we face from those who promote it
- Prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support and
- Work with sectors and institutions where there are risks of radicalisation that we need to address...[.]”

[Excerpted from 'Revised Prevent Duty Guidance: for Scotland': 2015]

[Additional documentation may be found at gov.uk](http://gov.uk)

### **Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008**

The Protection of Children Act 1978 prevents the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such



indecent photographs. Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.

The definition of 'photographs' include data stored on a computer disc or by other electronic means which is capable of conversion into an image.

It is an offence for a person to [...] distribute or show such indecent photographs or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160 of the Criminal Justice Act 1988 made the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment. The term "make" includes downloading images from the Internet and storing or printing them out.

#### **Protection from Harassment Act 1997**

Stalking, Offensive or threatening communications can also be charged under the Protection from Harassment Act. This can carry a sentence up to 5 years imprisonment.

#### **Sex Discrimination Act 1975**

Discrimination on the grounds of sex by dismissing an employee or submitting them to "any other detriment"

#### **Race Relations Act 1976**

As above, but on racial grounds

#### **Disability Discrimination Act 1995**

As above, but on grounds of disability

#### **Criminal Justice & Public Order Act 1994**

Intentional harassment for causing another person harassment, alarm or distress by using threatening, abusive or insulting words or behaviour

#### **Obscene Publications Act 1959 and 1964**

It is an offence to publish an obscene article or to have an obscene article in ownership, possession or control with a view to publishing it or, where the data is stored electronically, to transmit that data.

#### **Copyright, Designs & Patents Act 1988**



The "Copyright, Designs & Patents Act 1988" provides the same rights to authors of computer programs as literary, dramatic and musical authors have to their works. Those rights extend for the life of the author and for fifty years after the author's death.

Software is generally not sold outright to the purchaser. Instead the purchaser is granted the right to use it as laid down in the user licence. It is normally expected that only one person at a time will have access to and use the software concerned. A network licence may be purchased, normally at a reduced rate, for a defined number of users. A site licence may be available to cover all (unlimited) users within the premises.

It is thus illegal to make copies of software without the copyright owner's consent, or to duplicate software loaded on a hard disk for use on any other personal computer unless allowed for under the licence.

Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 2 years.

