

Data Protection Act 1998

WHAT IS PERSONAL DATA?

Personal data is any information that relates to a living individual.

HOW DOES IT AFFECT SCHOOLS?

Schools must register all personal data they hold and state the purposes for which it is required to be held. The fee for notification is now £35 and is renewable annually. Under the 1998 Act, as was the case with the 1984 Act, all processing undertaken by schools must be fair and lawful, accurate and up-to-date, and the data held must be adequate, relevant, not excessive and be held for no longer than is necessary. This means when personal data becomes out of date, or no longer relevant to the purpose for which it was originally collected, it must be destroyed. Holding on to the data may result in the school contravening the new Act.

CONDITIONS FOR PROCESSING PERSONAL DATA

Personal data should only be processed (that is, used) if one of several conditions apply including:

- _ an individual has given their consent
- _ the processing is part of a contract
- _ there is a legal obligation to process the data or
- _ the processing is necessary to protect the individual

If none of the conditions apply there are no legitimate grounds to process the data. Anyone found to be processing data in these circumstances would be contravening the Act. Contravening the Act is a criminal offence, which is punishable by a maximum fine of £5,000 in the Magistrates court and an unlimited fine in the Crown court.

NEW CATEGORY OF SENSITIVE DATA

The new Act also defines "sensitive personal data" for the first time including racial, ethnic origin, political affiliations, religious or other beliefs. This type of data demands greater protection and one of the following must be true before the data can be processed:

- _ an individual has given their explicit consent
- _ you have a legal requirement to process the data
- _ it is necessary to protect the vital interests of the individual

Explicit consent means fully informing the individual of the relevant facts in relation to the proposed processing and getting their written consent.

WHAT ABOUT PROTECTING PERSONAL DATA?

The new Act also makes it mandatory to ensure that appropriate technical and organisational measures are taken to prevent unauthorised access to or disclosure of data. This includes accidental loss or destruction of, or damage to, personal data. This means for example that sensitive data must be protected from unauthorised access by using password-based access control.

If a request for information under the Act is refused or ignored, the matter can be referred to the Data Protection Commissioner or an application for disclosure can be made to a court.

PRINCIPLES OF THE NEW ACT

There are eight over-arching principles of the 1998 Act:

- 1 Personal data shall be processed fairly and lawfully
- 2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4 Personal data shall be accurate and, where necessary, kept up to date

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

6 Personal data shall be processed in accordance with the rights of data subjects under the Act

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

WHAT HAPPENS IF THE ACT IS CONTRAVENED?

If anyone knowingly or recklessly contravenes the new Act, any individual suffering damage or distress as a result is entitled to claim compensation through the courts.

The courts may also prosecute the person responsible for committing the offence under the Act. Furthermore, if a Court rules that data relating to an individual is inaccurate, then the school can be required to delete or amend the data.

WHO IS RESPONSIBLE FOR DATA PROTECTION?

Everyone who handles personal data as part of their job needs to be aware of his or her responsibilities under the Data Protection Act, 1998. As was the case with the 1984 Act, individual employees are personally liable (a fine and a criminal record) for breaches of the Act if they disregard instructions given on the proper handling of personal data.

STAFF TRAINING – REQUIREMENTS OF THE ACT

All staff dealing with personal data should be aware of the requirements of the Act and be familiar with how to conform to these in their daily work. You may find it helpful for example to use this leaflet as a briefing note for new members of staff and as a 'refresher' document for existing staff.

PUBLICATION OF WEB PAGES

- Only access the Internet via a PC which has been expressly set up within the school for that purpose.
- Publication of personal information or images of individuals on any Web Site schools develop should only be done if the written consent of the individuals concerned has been given.

USE OF ELECTRONIC MAIL AND THE INTERNET - DATA PROTECTION REQUIREMENTS

The use of electronic mail and the Internet by schools also raises certain Data Protection issues. As an absolute minimum please bear the following points in mind:

- Do not include personal or confidential information in the text of emails (or as an email attachment) to be sent outside the school unless appropriate encryption is applied to protect it.

- Email should never be treated as a secure method of communication when dealing with personal data as defined by the Data Protection Act.

NEW CCTV CODE OF PRACTICE

CCTV cameras are increasingly being used by organisations for a variety of monitoring and surveillance purposes. In recognition of this the Data Protection Commissioner has issued a CCTV Code of Practice to comply with the provisions of the 1998 Data Protection Act. The code offers practical advice in helping schools to meet their legal obligations.

What does the Code of Practice cover?

The Code sets out the legal standards and provides guidance on good practice in addition to advice on practical matters such as suitable siting of CCTV cameras, procedures for informing people what is happening, guidance on what can happen to the images and how long you should retain them.

What is required to ensure schools' use of CCTV complies with the Act and the Code of Practice?

CCTV systems used on school premises must be operated in accordance with the provisions of the Data Protection Act, 1998. Responsibility for adhering to the relevant requirements here rests with the individual school concerned.

Schools have a legal duty to notify the Data Protection Commissioner of the purposes for which the CCTV equipment is used. Appropriately worded signs must also be on display on the school site pointing out that such equipment is in use and the purpose for it being in operation.

The recommended wording for a notice is 'CCTV surveillance equipment is in operation in this area. Images are being recorded for the purposes of crime prevention, for ensuring the safety of School employees and visitors, and for protecting School premises and property.

The notice should also include both details of the organisation responsible for the scheme e.g. the name of the school and the specific contact point for further information (usually the head teacher).

ACCESS TO PERSONAL DATA – PUPIL RIGHTS

The Data Protection Act gives all school students, regardless of age, the right of access to their school pupil records. Requests to see or receive copies of records should be made in writing to the head teacher. In addition to the right to be given a copy of the educational record, Student's are entitled to be given a description of the personal data which makes up the record, together with details of the purposes for which the data are processed, the sources of the data (if known) and the individuals or organizations to which the data may have been disclosed.

A period of up to 15 school days is allowed in which to respond to a subject access request. (The equivalent period for other types of record is up to 40 days.) If asked to provide a hard copy of the record, a fee may be charged according to the number of pages. Students may be asked for information to verify their identity if necessary, for instance in the case of former pupils who may not be currently known to the school. They may also be asked for information necessary to locate the data held about them. For instance a student may be asked to supply the dates between which he or she attended the school.

While in principle students have a right of access to the whole of their educational records, in exceptional cases some information may be withheld. The main exemptions are for information which might cause harm to the physical

or mental health of the student or a third party, information which may identify third parties (for example other pupils, although not teachers), and information which forms part of some court reports. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.

If students are incapable of understanding or exercising their own rights under the Data Protection Act, (for instance because they are too young), parents can, of course, make subject access requests on their behalf.

ACCESS TO PERSONAL DATA – PARENTAL RIGHTS

In addition to the subject access right which can be exercised by pupils or by parents acting on behalf of pupils, parents have their own independent right of access to the official educational records of their children. In essence the information to which parents are entitled and the exemptions are the same as for pupils, although there is no parental right of access to information which does not form part of the official record. Requests to see or receive copies of the educational records of their children should be made in writing.

WHAT ABOUT MANUAL FILING SYSTEMS DATA?

A major change under the new Act is that it now makes certain data held in manual or paper form subject to the data protection rules. For the first time individuals whose personal information is recorded manually will, in some cases, have a right to see that information and make corrections if necessary.

WHAT IS A STRUCTURED MANUAL FILING SYSTEM?

This means any set of information relating to an individual that is readily accessible either by reference to the individual or criteria relating to the individual.

The Data Protection Act, 1998 came into force on 1st March, 2000. This leaflet provides a summary of its key points and operating principles. Please use it as a guide to ensure that your school adheres to legal requirements in this important area. The new Act carries forward elements from the previous Data Protection Act, introduced in 1984, and imposes stringent conditions on the way 'data controllers' such as schools hold or process personal data.



Liz Johnston belb October 2004
Board of Governors Awareness Sessions.