The Attic
Data Protection Policy

Date of policy	June 2017
Date presented to Management Committee	July 2017
Date ratified by Management Committee	July 2017
Date for review	July 2018

The Data Protection Act 1998 places duties and obligations on schools in relation to the processing of personal data.

Significant elements of the Data Protection Act 1998 come into force on the 24th October 2001. The new Act replaces the 1984 Data Protection Act and provides enhanced rights for data subjects whilst also increasing the responsibilities of the data controller.

The Data Protection Registrar has now become the Information Commissioner with revised powers and duties.

Rules for Processing Personal Data

Personal data is any information relating to an identifiable living individual and covers facts or opinions about an individual.

The definition of processing is fairly wide and includes obtaining, sorting, retrieving, using, disclosing and destroying personal data.

Anyone processing personal data must comply with the eight enforceable principles of good practice (see below). Personal data must be collected and handled in a way that complies with the Act. This imposes a duty on the centre to ensure that individuals must be aware of the uses that will be made of the information that they supply and give their consent to this. Where the use is obvious (e.g. name and address for correspondence purpose) or there is a statutory duty or legal requirement to process the data, then consent does not need to be explicitly obtained.

Where there is no clear purpose then consent should be obtained (in the case of students over 13 years old, they must be approached directly) and the individual must be made aware of the purpose for which the data will be used. In addition to obtaining consent the data must be used only for those purposes that the Pupil Referral Unit has notified the Management Committee of. If there is a new purpose, or a change to an existing purpose, the Management Committee must be notified immediately. Processing of data cannot begin until the Management Committee has accepted this notification.

When using a form to collect information it must state clearly the purpose for which you will be using the information. If you are explaining the purpose to the individual you must be sure that they understand what use you will be making of their information.

If you collect any 'sensitive' information, including physical or mental health or condition, you must have explicit consent to process this information. 'Explicit consent' means the individual must be fully informed about the purposes for which you will use the information, who it will be disclosed to, how long you intend to keep it and have the option to remove their consent at any time. They should sign the form to show their agreement. You can also only collect relevant information, no extras just because it could be useful.

The Eight Data Protection Principles

1. Fairness and Legality

- Personal data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed.

- Personal data shall not be processed unless:

  a) at least one of the conditions in Schedule 2 is met, and

  b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

  (see Appendix A for Schedules 2 & 3)

2. Purpose

- Personal data can only be obtained for one or more specified and lawful purpose, and shall not be processed further in any manner incompatible with that purpose.

3. Adequacy

- Personal data has to be adequate, relevant and not excessive in relation to the purpose for which the data is meant to be processed. You cannot collect information that you do not need.

4. Accuracy

- Personal data should be accurate and up-to-date and should be amended if it is found to be incorrect.

5. Length of use

- The Act requires that personal data must not be kept any longer than is necessary for the purpose for which it was obtained. It cannot be used for something else or passed on more widely without the individual knowing.

6. Access Rights

- Data subjects have the right to access their personal data and can block any processing that causes or is likely to cause them 'distress'. They can insist that their data is not used for marketing purposes and they have the right to know the rules behind any automated decision making process.

7. Security

- The Act requires organisations to take appropriate measures to prevent unauthorised processing of personal data and to protect personal data against loss, damage or destruction. This extends to third party processors.

8. Transfer outside the EU

- Personal data cannot be transferred to a country outside the EU unless that country has in place a level of data protection comparable to that in the EU.

Personal Data

Personal data is any information by which a living individual can be identified.

Some types of personal data are:

- Name
- Address
- Date of Birth/Age
- Financial details
- Employment details
- Political party membership
- Family circumstances
- Telephone number

Sensitive Personal Data

Sensitive data can only be processed under strict conditions, which include:

- Having the explicit consent of the individual (any person over 13 years of age).
- Being required by law to process the data for employment purposes.
- The information is needed in order to protect the vital interests of the data subject or another.
- Dealing with the administration of justice or legal proceedings.

Sensitive personal data covers the following areas:

- Disability
- Racial origin
- Political opinions
- Trade Union membership
- Sexual life
- Religious beliefs or other beliefs of a similar nature
- Court proceedings, criminal convictions or allegations
- Physical health records
- Mental health records

Manual Data

Manual data comprises of structured records about individuals that are stored on paper. This includes manual data that is recorded as part of a 'relevant filing system' where records are structured either by reference to an individual or by reference to criteria relating to individuals.

Security

Educational establishments as "data controllers" are required to tell the Management Committee what they are doing about security as part of their registration/notification. The Headteacher must adopt an Information Protection and Security Policy to ensure compliance with the Act. The Act does not specify the measures that should be taken, this is left to the individual workplaces, who should in each case consider what measures are available and their cost.

Whilst security measures can never guarantee 100% protection they should be able to reduce the risk to the confidentiality, integrity or availability of data to an acceptable level, any breaches of security should be investigated.

The following areas should be considered by educational establishments in relation to security.

Access to Personal Data

- Who can access the information?
- Who can give information and to whom?
- How will the centre deal with subject access rights?

Physical Security

- All premises should enable information processing to take place in a secure environment.
- Filing cabinets containing personal data must be locked outside of normal working hours and nominated staff must hold keys securely.
- Electronic files on the server should be password protected and passwords should be changed on a regular basis. Electronic files ideally should be stored within the Attic pupil Referral Unit Cloud. All such data should be backed up regularly.
- If data is to be taken from the office (e.g. to do work at home) then the data must be secure at all times whilst in transit and at any location.

Personnel

- Emphasis should be placed on the responsibility of all staff to adhere to their duty of confidence and enforce the security procedure chosen.
- Measures to ensure the reliability of staff through selection, awareness, education and supervision, including non-permanent staff with permitted access to personal data.

- Audit trails that are sufficiently detailed and kept for long enough to enable a comprehensive audit of accesses to a system and failed attempts. This will ensure that staff are aware that the actions for which they are accountable can be traced back to them.

Equipment

- IT should be installed in accordance with the manufacturers instructions and used in a manner that will ensure safe and secure processing.

- IT equipment should be sited in order to minimise risk of damage, theft or unauthorised access.

- Equipment should be covered by a maintenance agreement and should be maintained in accordance with manufacturers guidelines and specification.

- All repairs and servicing should only be undertaken by qualified personnel.

- A record should be kept of all faults and any work undertaken.

- Equipment used for processing or storing personal information should undergo a risk assessment before being released to an external organisation.

- Users should ensure that unattended equipment is suitably protected against unauthorised access. In the case of sensitive information, users should ensure that they log off the system. In other circumstances a suitable lock such as a password protected screen saver could be used with automatic activation after a maximum delay of 10 minutes.

Retention and Disposal

Establishments need to consider how and where material is held, for how long and how it will be disposed of.

- Paper containing personal data should be shredded or pulped under secure conditions.

- Hard disks will continue to hold data even though the relevant files have been deleted. If you are disposing of a PC you must ensure that the hard disk has been wiped clean.

Subject Access Rights

The Data Protection Act 1998 gives all individuals who are the subject of personal data (“data subjects”) a general right of access to personal data that relates to them. These rights are known as "subject access rights". Requests for access to records and for other information about those records are known as "subject access requests." Personal data may take the form of computerised or paper records.

The Act also sets out specific rights for school students in relation to educational records held within the state education system whether these are held in computerised or paper form. Educational records are the official records for which head teachers are responsible.

The rights of students lie alongside the rights of parents to obtain copies of the educational records relating to their children.

Young People Rights

The Data Protection Act gives all young people, regardless of age, the right of access to their school records. Requests to see or receive copies of records should be made in writing to The Headteacher.

In addition to the right to be given a copy of the educational record, students 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 organisations to which the data may have been disclosed. Copies of pupil reports now form part of the pupil's educational record.

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 (4p a copy A4 – 3p a copy over 100). Young people may be asked for information to verify their identity if it is necessary, for instance in the case of former pupils who may not be currently known to the centre. They may also be asked for information necessary to locate the data held about them. For instance a young person may be asked to supply the dates between which he or she attended the centre.

Whilst in principle young people 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 that might cause harm to the physical or mental health of the student or a third party, information that may identify third parties (for example other young people, although not teachers), and information that 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. If young people 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.

Parent's Rights

In addition to the subject access rights, that 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 under the Education (Pupil Information) (England) 2000 Act. This Act states that parents are entitled to have their child's educational records disclosed to them, free of charge, within 15 days of making a written request. If a hard copy is required the subject access fee can apply. Parents have no rights of access to information which does not form part of the official record or have a right of redress under the Data Protection Act unless he or she is acting on behalf of their child.

If a parent is not given a copy of his or her child's records, in the first instance he or she should contact the management committee and, after that, the DCFS or, as a last resort, the courts.

Because parents have an independent right of access to pupil records, the young people themselves have no right to prevent their parents from obtaining a copy of their school records.

Registration Under the New Act

Under the 1998 Act only one registration will be required and will cover the Headteacher.

Under the 1998 Act 'notification' is the term used to describe registration being the process by which a data controller's details are added to the Data Protection Register. The fee for notification under the new Act is £35 per annum.

Offences under the Data Protection Act

Failure to Register

It is a criminal offence for a data controller not to register with the Data Protection Commissioner. It is also an offence to fail to notify the Commissioner of any changes that have been made to the processing of personal data. Fines may be imposed on offenders of up to £5,000 in the magistrate's court and may be unlimited if convicted in the crown court.

Procuring and Selling Offences

It is a criminal offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data or to disclose it without the permission of the data controller. It is also a criminal offence to access personal data or to disclose it without proper authorisation. This covers unauthorised access to and disclosure of personal data.

Personal Liability

The Data Protection Act provides that where an offence has been committed by a company, and has been committed with the consent or is attributable to negligence on the part of an officer of the company, he or she, as well as the company may be prosecuted. A successful prosecution could result in a prison sentence of up to five years.

In practice the Data Protection Commissioner will wish to ensure that data controllers comply with the requirements of the new Act without recourse to the courts. In the case of schools compliance may be achieved through registration and by implementing some basic procedures relating to security and the processing of data. Whilst the new Act does impose some new duties and responsibilities, most of these are in line with existing good practice in terms of maintaining the confidentiality and security of all personal data.

The Education Departmental Data Protection Co-ordinator will be available to provide advice and assistance where this is required. Nevertheless, it is important to note that the responsibility for compliance lies with each individual school/educational establishment.

Appendix A - Extracts from the Data Protection Act 1998

Conditions for Processing

(Schedule 2 of Act)

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies): -

- The data subject has given their consent.
- The processing is necessary: -
  a) for the performance of a contract to which the data subject is a party, or
  b) for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The processing is necessary in order to protect the vital interests of the data subject (life and death situations).
- The processing is necessary: -
  a) for the administration of justice,
  b) for the exercise of any functions conferred by or under any enactment,
  c) for the exercise of any functions of the Crown, a Minister or the Crown or a government department, or
  d) for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third part or parities to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

Sensitive Personal Data

Categories of sensitive personal data, namely, personal data consisting of information as to: -

a) the racial or ethnic origin of the data subject,
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether they are a member of a trade union,
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by them of any offence, or
h) any proceedings for any offence committed or alleged to have been

committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Conditions for Processing Sensitive Data (Schedule 3 of the Act)

At least one of these must be satisfied, in addition to at least one of the conditions in schedule 2, before processing of sensitive personal data can claim to have been lawful in accordance with the First Principle.

- The data subject has given the explicit consent to the processing of the personal data.

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

- The processing is necessary: -
  a) in order to protect the vital interests of the data subject or another person, in a case where: -

    - *- consent cannot be given by or on behalf of the data subject, or*

    - *- the data controller cannot reasonably be expected to obtain the consent of the data subject, or*

  b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- The processing: -
  a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade-union purposes and which is not established or conducted for profit,
  b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
  c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and
  d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

- The processing: -
  a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings).
  b) is necessary for the purpose of obtaining legal advice, or
  c) is otherwise necessary for the purpose of establishing, exercising or defending legal rights.

- The processing is necessary: -
  a) for the administration of justice,
  b) for the exercise of any functions conferred by or under any enactment, or

c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

- The processing is necessary for medical purposes and is undertaken by:
  a) a health professional (as defined in the Act), or
  b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

- The processing:-
  a) is of sensitive personal data consisting of information as to racial or ethnic origin,
  b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
  c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

- The personal data are processed in circumstances specified in an order made by the Secretary of State.

The Secretary of State may by order specify circumstances in which such processing is, or is not, to be taken to be carried out with appropriate safeguards for the rights and freedoms of data subjects.