Data Protection – a model policy for schools

THIS DOCUMENT SHOULD BE AMENDED AND APPROVED BY THE GOVERNING BODY. IT WILL REQUIRE UPDATING AS GUIDANCE ON DATA PROTECTION FURTHER DEVELOPS.

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- the rights in respect of people whose data is being held and processed by the school (this includes pupils, parents, staff and governors).

1.1. Safeguarding

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.
Keeping children safe in Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.2. It is a statutory requirement for all schools to have a Data Protection Policy:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools

In addition to this policy, schools should have:

- **Retention Information** - details on how long all records are retained
- **Information Asset Audit** - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
- **Privacy Notices -** for pupils, parents, staff and governors
- **Registered with the ICO**

This policy will link with the following:

- Safeguarding Policy
- Staff AUP/Code of Conduct
- Photographic Policy
- Photographic Consent Forms

1.3. Definitions

- Personal Data - information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held. (Note that information can be in any form - written, on a PC e.g. names, addresses, photos.)
- Data Processor – a person who handles the data including filing or storing it.
- Data Subject – the person about whom personal data is processed or kept.
- Data Controller - the person or organisation who determines the "how and what" of data processing in an organisation.

1.4. Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

2. Lawful Basis for Processing Data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary. Your legal advisor will be able to identify individual statutes if required.

2.1 Age

Children under the age of 13 are not usually considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians can do this on their behalf, providing this is in the best interests of the child. See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/ Children should be provided with age appropriate advice about how their data is used.

2.2 Consent

If there is a lawful basis for collecting data, then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

3. RIGHTS

GDPR provides the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Different rights attach to different lawful bases of processing:

	Right to erasure	**Right to portability**	**Right to object**
Vital Interests	✓	**X**	**X**
Legal Obligation	**X**	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interests	✓	**X**	✓
Contract	✓	✓	**X**
Consent	✓	✓	**X** but right to withdraw consent

3.1. The right to be informed – *See Privacy Notices section 6.2*

3.2. The right of access

Depending on the age of the pupil, there are two legal basis for pupils or parents to request access to their data – a Subject Access Request or a request under the 2005 Education Regulations.

3.2.1. Subject Access request under GDPR

GDPR gives individuals the right to access any data that an organisation holds on them. Normally this has to be completed within 30 days without charge. Further guidance is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ Schools should be aware that guidance from the ICO highlights the rights of the child. *"Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident*

that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child."

3.2.2. In maintained schools, parents have another statutory right to access their children's educational record

This is part of the Education (Pupil Information) Regulations 2005. This applies to all children under 16 years and has to be completed in 15 working days. See https://ico.org.uk/your-data-matters/schools/pupils-info/

3.2.3. Information which may be withheld

On some occasions records could contain information which ***"is likely to cause significant harm to the physical or mental health of the child or others",*** for instance, if a child makes a disclosure of abuse. In these circumstances, the data should not be released and the pupil/parent does not need to be informed of its existence. If in doubt seek legal advice.

3.3. The right to erasure

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Your legal advisor will be able to support with information about which data can continue to be legally held if a data subject asks to be 'forgotten'. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that, where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above), there is no right to erasure – however, this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

4. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach", which could result in legal action against the school. The loss of sensitive, or "special category", personal data is considered much more seriously and the sanctions may well be more punitive.

4.1. Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils-/students, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

4.2. Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a child, his or her family or a member of staff
- medical information about a child or member of staff (SEND)
- (some information regarding safeguarding will also fall into this category)
- staffing e.g. Staff Trade Union details.

Note – See section on Sharing Information.

4.3. Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources and other information about the school which does not relate to an individual. Some of this

data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

5. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection; they should appoint a Data Protection Officer to manage data.

5.1. Risk Management – Roles: *Data Protection Officer*

The school should have a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

In some schools, other staff may have been delegated responsibility for particular issues, for instance the handling of SEND information.

5.2. Risk management - Staff and Governors Responsibilities

Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

6. Legal Requirements

6.1. Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration: https://ico.org.uk/for-organisations/data-protection-fee The register may be checked by visiting https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

6.2. Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the school **must** inform parents/carers of all pupils/students and staff of the data they collect, process and hold on the pupils/students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. More information about the suggested wording of privacy notices can be found on the DfE website:
http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

Privacy notices should be made available to pupils, parents and carers, for instance, by publishing on the school website and making a paper copy available when children first register for school.

Children should be provided with age appropriate information about how their data is being used.

7. Transporting, Storing and Disposing of personal Data

7.1. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

7.1.1. Technical Requirements

The school will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

The school/academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (The school will need to set its own policy, relevant to its physical layout, type of IT systems etc. Schools need to be aware of a significantly higher risk of a data loss, and should ensure that they can recover from a cyber-attack.)

7.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- the school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices
- *We would advise that…* Only encrypted removable storage purchased by the school is allowed to be used on school computers.

7.1.3. Passwords

All users will use strong passwords (14 Characters including a Capital letter, number and symbol) which must be updated occasionally. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

7.1.4. Images

Images will be protected and stored in a secure area. See school Photographic Policy.

7.1.5. Cloud Based Storage

The school/academy has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data. See advice from the DfE below:

https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

7.2. Third Party data transfers

As a Data Controller, the school/academy is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party, as well as data processing agreements.

7.3. Retention of Data

The guidance given by the Information and Records Management Society – Schools records management toolkit can be used as a basis for determining how long records are kept. This school retention information should be available to data subjects on request.

Personal data that is no longer required will be destroyed and this process will be recorded.

7.4. Systems to protect data

7.4.1. Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

- paper based safeguarding chronologies will be in a locked cupboard when not in use
- class lists used for the purpose of marking may be stored in a teacher's bag.

Paper based personal information sent to parents (will be checked by office manager before the envelope is sealed).

7.4.2. School Websites

Uploads to the school website will be checked prior to publication, for instance:

- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded.

7.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

Where technically possible, all e-mail containing sensitive information will be encrypted by attaching the sensitive information as a word document and encrypting the

document/compressing with 7 zip and encrypting - the recipient will then need to contact the school for access to a one-off password [*or when available* using the security features available in Office 365]).

8. Data Sharing

8.1. Sharing with the LA and DfE

The school is required by law to share information with the LA and DfE. Further details are available at: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

8.2. Safeguarding

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Durham LSCB provides information on information sharing at: http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

8.3. Transfer of Safeguarding and SEND records when a pupil moves school

The following is an extract from keeping Children safe in Education Sept 2018.

- Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.

- Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.

- In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

9. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach, the data protection officer will inform the head teacher and chair of governors.
- When a personal data breach has occurred, the school must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if the school decide not to report the breach, they need to be able to justify this decision, and it should be documented.
- The school must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the school takes longer than this, they must give reasons for the delay.
- If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

Any report about a data breach must include:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; *and*
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; *and*
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.

Further details are available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

10. Policy Review Reviewing

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

Date: September 2020 Review date September 2022

Signed:
J. Waine

Adopted by the Governing Body on _____

The Data Protection Officer is Martin Orwin

Appendix 1 - Links to Resources and Guidance

ICO Guidance
Specific information for schools is available here. This includes links to guides from the DfE.
http://ico.org.uk/for_organisations/sector_guides/education

Specific Information about CCTV.
https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Information and Records Management Society – schools records management toolkit
A downloadable schedule for all records management in schools.
http://irms.org.uk/page/SchoolsToolkit

Disclosure and Barring Service (DBS)
Details of storage and access to DBS certificate information.
https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information

DFE
GDPR Toolkit
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Safeguarding
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
and
https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Appendix 2 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR
All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:
The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:
General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:
General information note from the Information Commissioner on publication of examination results.

Education Act 1996:
Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:
Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972:
Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:
Retention of school admission and exclusion appeal papers and other pupil records.