Policy Number:

Policy Title: Data Protection

Author:

Last updated:

Data Protection (GDPR) Policy

Date adopted: April 2019

Reviewed: November 2021

Review date: Bi-Annually

1. Aims and Objectives

It is a statutory requirement for all schools to have a Data Protection Policy. 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
- how staff, parents and pupils can access personal data

2. Data Protection Principles

In accordance with Article 5 of the GDPR, Hall Grove School will ensure 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 purpose 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 organisation measures. Hall Grove School (the controller) shall be responsible for, and be able to demonstrate, compliance with the principles, i.e. its policies and systems comply with requirements of GDPR.

3. Lawful Basis for processing data

The vast majority of information that the school will collect and process is required to enable the school as the data controller to perform tasks carried out in the public interest or in the exercise of official authority vested in the school. There are other reasons that may make processing necessary, such as a specific legal obligation applying to the data controller.

If there is a lawful basis for collecting data, then consent to collect data is not required. Consent is obtained when there is no legal reason for processing, such as for images used in school publicity or social media feeds. The consent will be transparent, revocable, and will be on a "opt-in" basis. Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. Over the age of 13, this responsibility is transferred to the child and parents will not have responsibility for their child's data. A privacy notice which explains the lawful basis for processing the data and the rights of the individual is provided on the school website.

Rights

The GDPR provides for 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	o	x	x
Legal Obligation	x	x	x
Public Task	x	x	o
Legitimate Interests	o	x	o
Contract	o	o	x

Consent	o	o	x
			(But right to withdraw consent)

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. 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

GDPR defines different types of data and prescribes how it should be treated.

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 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" 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

4.3 Other types of Data not covered by the Act

This is data that does not identify a living individual and could 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).

5. Responsibilities

The Headmaster has overall responsibility for Data Protection, although everyone in the school has the responsibility of handling personal information in a safe and secure manner

6. Legal Requirements

6.1 Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner

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

The school's Privacy Notice is published on the school website and provides the required information for parents/carers of all pupils and staff of the data we collect, process and hold on the pupils, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. local authority, DfE, etc.) to whom it may be passed as well as the data subjects' rights under GDPR.

7. Transporting, Storing and Disposing of personal Data

7.1 Information security – Storage and Access to Data

7.1.1 Technical Requirements

- The school ensures that ICT systems are configured so that the existence of protected files is hidden from unauthorised users and that users are 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 unattended (even for very short periods).
- 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 (i.e. owned by the users) must not be used for the storage of personal data.
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

7.1.2 Portable Devices

When personal data is stored on any portable computer system:

- The data must be encrypted and password-protected.
- The device must be password-protected.
- The data must be securely deleted from the device in accordance with school policy once it has been transferred or its use is complete.
- Data storage of personal information on removal media e.g. USB, portable hard drive, is not allowed, even if encrypted.
- Staff may only use removable media e.g. USB, portable hard drive to transfer non-personal information e.g. for use in lesson planning.

7.1.3 Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared.

7.1.4 Images

- Images of pupils will only be processed and transported by use of authorised agents of the school and permission for this will be obtained in the privacy notice or other photographic permission notice.
- Images will be protected and stored in a secure area.

7.1.5 Cloud Based Storage

- The school has a clear policy and procedures for the use of "Cloud Based Storage Systems" 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.

7.2 Third Party data transfers

As a Data Controller, the school is responsibility 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 guidelines given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded. Persuading staff to reduce the quantity of personal information they have collected over time should be regarded as an important priority.

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: 1. Paper-based safeguarding chronologies will be in a locked cupboard when not in use 2. Class lists used for the purposes of marking may be stored in a teacher's bag
- Paper-based personal information sent to parents will be checked 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

- Where technically possible, all e-mail containing sensitive information must be encrypted.
- The use of a secure e-mail system allows for secure communication.

8. Data Sharing

The school is required by law to share information with the local authority and DfE as well as other government bodies.

9. Data Breach Procedures

In the event of a data breach, the member of staff who becomes aware of the breach must inform the Headmaster as soon as practically possible. The Headmaster will take such further steps as are required to prevent further breaches and to notify the appropriate bodies and data subject(s) concerned.

10. Policy Review Reviewing

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

Links to resources and guidance

ICO Guidance on GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for_organisations/sector_guides/education

Specific information for schools is available here. This includes links to guides form the DfE

http://ico.org.uk/for_organisations/data_protections/topic_guides/cctv

Specific information about CCTV

Information and Records Management Society – Schools records management toolkit
http://irms.org.uk/page/SchoolsToolkit

A downloadable scheduled for all records management in schools

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

Details of storage and access to DBS certificate information

DfE Privacy Notices

https://www.gov.uk/government/pulications/data-protection-and-privacy-privacy-notices

DfE Use of Biometric Data

https://www.gov.uk/government/publications/protection-of-biomentric-information-ofchildren-in-schools

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 regulated 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 and 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.

Reviewed: November 2021