St Hilda's School
HARPENDEN
Caring, Curious & Confident

DATA PROTECTION POLICY

Name of Policy	Data Protection Policy
Reviewed by	Dan Sayers Daniel James
Review Date	December 2025
Next Review Date	December 2026
To be Read in Conjunction with	• School's Privacy Notice • Complaints Policy
Legislation Referenced	• Data Protection Act 2018 • UK General Data Protection Regulation • Department of Education Disposal of Records Schedule.

Unless otherwise stated, all Policies of St Hilda's School apply to the school in its entirety. This comprises all staff and pupils in the Early Years Foundation Stage (EYFS), the Junior School (Key Stage 1) and the Senior School (Key Stage 2).

CONTENTS

1. INTRODUCTION

At St Hilda's we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

The School is subject to the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) which implements into English law the EU General Data Protection Regulation with various amendments post-Brexit. These impose obligations on the School as a data controller in relation to the protection, use, retention and disposal of Personal Information. This Policy sets out the procedures that are to be followed when dealing with Personal Information and applies to all Personal Information processed by or on behalf of St Hilda's.

This policy gives important information about:

- the data protection principles with which St Hilda's must comply.
- what is meant by Personal Information and Special Category Data.
- how we gather, use and (ultimately) delete Personal Information and Special Category Data in accordance with the data protection principles.
- where more detailed Privacy Information can be found, e.g. about the Personal Information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept.
- your rights and obligations in relation to data protection.
- the consequences of our failure to comply with this Policy.

Please refer to the School's privacy notices which contain further information regarding the protection of Personal Information in those contexts.

2. DATA PROTECTION PRINCIPLES

The UK GDPR sets out the following principles with which any party handling Personal Information must comply.

All Personal Information must be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes only, and not be 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 not be considered to be incompatible with the initial purposes.
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that inaccurate Personal Information is deleted or corrected without delay.
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed; Personal Information may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, subject to implementation of the

appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the individual.
- processed in a manner that ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. DATA PROCESSING

Under the UK GDPR, there are 6 lawful bases on which personal data (see Appendix 1 for definition) is permitted to be processed.

The lawful bases are:

- **consent** – where this basis is the most appropriate and the school is able to give the individual concerned a real choice in the use of their data. Parental consent will be obtained for any child aged under 13 years old.
- **contract** – where use of the data is necessary for a contract the school has or will have with the individual concerned.
- **legal obligation** – where use of the data is necessary to permit the school to comply with the law.
- **vital interests** – where use of the data is necessary to protect an individual's life.
- **public interest** – where use of the data is necessary to permit the school to carry out a task in the public interest or its official functions, and that task or function has a clear basis in law.
- **legitimate interests** – where use of the data is necessary for the school's or a third party's legitimate interests (unless there's a good reason to protect the individual's personal data that overrides those legitimate interests).

Except where the processing is based on consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Under UK GDPR, there are 10 additional conditions for processing Special Category Data. See ICO's guidance for full details:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/

4. RIGHTS OF THE INDIVIDUAL

The UK GDPR states that individuals have the following rights in respect of the processing of their Personal Information:

- The right to be informed: The School will keep individuals informed of its processing activities through its privacy notices.
- The right of access: An individual may make a subject access request ("SAR") at any time to find out more about the Personal Information which the School holds on them. All SARs must be forwarded to the Headteacher. The School is required to respond to a SAR within one month of receipt but this can be extended by up to two months in the case of complex

and/or numerous requests and, in such cases, the individual will be informed of the need for such extension. The School does not charge a fee for the handling of a straightforward SAR. The School follows the ICO's guidance on how to deal with a request for information.

- The right to rectification: If an individual informs the School that Personal Information held by the School is inaccurate or incomplete, the individual can request that it is rectified.
- The right to erasure: An individual is entitled to request that the School ceases to hold Personal Information it holds about them. The School is required to comply with a request for erasure unless the School has reasonable grounds to refuse.
- The right to restrict processing: An individual is entitled to request that the School stops processing the Personal Information it holds about them in certain circumstances.
- The right to data portability: An individual has the right to receive a copy of their Personal Information and use it for other purposes.
- The right to object: An individual is entitled to object to the School's processing of their Personal Information.
- Rights in relation to automated decision making and profiling: An individual has the right to challenge any decision that is made about them on an automated basis (subject to certain exceptions).

5. DATA PROTECTION OFFICER

The Business Manager is the Data Protection Officer and will monitor adherence to this policy.

6. STAFF RESPONSIBILITIES

- No member of staff is permitted to remove unsecured personal data from the School premises, whether in paper or electronic form and wherever stored, without prior consent of the Data Protection Officer.
- Use of personal email accounts or unencrypted personal devices by staff for official School business is not permitted.
- No member of staff should provide personal data of pupils or parents to third parties, unless there is a lawful reason to do so.
- All staff must handle personal data with which they come into contact in a fair, lawful, responsible and secure manner, in accordance with the relevant School policies and procedures. They should:
  - make sure they have a legitimate need to process the data.
  - check that any data they store is needed to carry out necessary tasks.
  - identify any risks.
  - understand the governance arrangements that oversee the management of risks.

7. DATA RETENTION AND DISPOSAL

The longer that Personal Information is retained, the higher the likelihood of accidental disclosure, loss, theft and/or information growing stale. Any Personal Information kept by the School is managed in accordance with the Department of Education Disposal of Records Schedule. All data that is no longer required is destroyed / removed in line with regulatory guidance. Paper records are shredded using a cross-cutting shredder.

A review is conducted at the end of each academic year to determine what data needs to be retained or disposed of.

8. DATA BREACH

A data breach is any (potential) unintended loss of control over or loss of Personal Information within the School's environment. It is a security incident that results in personal data a school holds being:

- lost or stolen
- destroyed without consent
- changed without consent
- accessed by someone without permission

Data breaches can be deliberate or accidental.

Preventing a data breach is the responsibility of all the School staff and its workforce.

In the event of a serious data breach involving personal data, the Data Protection Officer must report the breach to the Information Commissioner. A serious breach is a breach that interferes with the rights and freedoms of the data subject. Serious breaches must be reported to the ICO within 72 hours of becoming aware of the breach, where feasible.

9. THIRD-PARTY SERVICES AND SUBCONTRACTING

The School may decide to contract with a third party for the collection, storage or processing of data, including Personal Information. If the School decides to appoint a third party for the processing of Personal Information, this must be regulated in a written agreement in which the rights and duties of the School and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organisational security measures required in this Policy, and provide sufficient guarantees with respect to the protection of the personal rights and the exercise of those rights. The subcontractor is contractually obligated to process Personal Information only within the scope of the contract and the directions issued by the School.

10. COMPLAINTS

Complaints will be dealt with in line with the School's Complaints Policy. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, quoting St Hilda's reference Z8475697.

APPENDIX 1

DEFINITIONS

“consent” is any freely given, specific and transparently, well-informed indication of the will of the individual, whereby the individual agrees that his or her Personal Information may be processed. Particular requirements about consent can arise from the respective national laws.

"Personal Information" (sometimes known as “personal data”) means any information relating to an identified or identifiable living person. An identifiable person is one who can be identified, directly or indirectly — in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In a school, examples of personal data include:

- identity details (for example, a name, title or role)
- contact details (for example, an address or a telephone number)
- information about pupil behaviour and attendance
- assessment and exam results
- staff recruitment information
- staff contracts
- staff development reviews
- staff and pupil references

“processing” means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with Personal Information.

"Special Category Data" (sometimes known as “sensitive personal data”) means Personal Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and the processing of data concerning health, sex life or sexual orientation. In a school, it would be best practice to also treat as special category data any personal data about:

- a safeguarding matter
- pupils in receipt of pupil premium
- pupils with special educational needs and disability (SEND)
- children in need (CIN)
- children looked after by a local authority (CLA)