Data Protection Policy

2024-2025

Approved by:	Headteacher	**Date: September** 2024
Last reviewed on:	September 2024	
Next review due by:	September 2025	

Introduction

Hale Prep School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use the information to ensure that the school complies with its statutory obligations.

Hale Prep School is responsible for and subject to laws and regulations that apply to the security and processing of records, data and personal information.

Data Protection Administrator

In conjunction with the Senior Management Team, the Data Protection Administrator, Mrs Ruth Vayro, is responsible for ensuring that all records are securely maintained and that their access and use comply with the relevant statutory requirements.

The Senior Management Team shall ensure that all those employed by or working for the school know these guidelines and their duties and responsibilities. Hale Prep School has complied with the requirement to register with the Information Commissioner's Office (ICO).

Purpose

This policy intends to ensure that all personal information is handled correctly, securely, and by all statutory requirements. It will apply to information regardless of how it is collected, used, recorded, stored and destroyed and whether it is held in paper files or electronically. All staff collecting, processing and disclosing personal data will be aware of their duties and responsibilities by adhering to these guidelines. Personal information or data is defined as data which relates to a living individual – who can be identified from that data – or information held.

Data Protection Principles

At all times, the following principles are adhered to:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes

- Personal data shall be processed by the GDPR
- Personal data shall be kept secure, i.e. protected by an appropriate degree of security
- Personal data shall not be transferred to a country or territory outside the European Economic Area

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform the individuals why and when the information is being collected
- Request permission to share information
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Request (SAR).
- Check the quality and the accuracy of the information it holds
- Ensure the information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so

Data Storage and Security

We look after your data by having security appropriate for its nature and the harm that might result from a security breach. This shall include but not be limited to:

- Keeping all school buildings and access to them secure
- Ensuring computer equipment and all physical records are secured in rooms where they are locked away, only accessible by those authorised to access them.
- Ensuring that all those with access to the school's computer systems or devices are trained in computer and data security and aware of the importance of maintaining secure passwords and not disclosing or sharing their information for unauthorised purposes.

- All staff or otherwise authorised persons accessing school records and data shall be fully referenced and checked (including but not limited to DBS checks).
- Communicating regularly with staff and students about the importance of data protection and security. • Making it a serious disciplinary offence for failing to comply with this or similar policies.

Requests

Ensure our staff are aware of and understand our policies and procedures. Complaints.

The school's complaints policy will deal with complaints.

Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Contacts

If you have any enquiries about this policy, please get in touch with Mrs Vayro - who will act as the contact point for any subject access requests. Further advice and information is available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 1231113.

Policy Review

This policy will be reviewed every two years and updated in line with legislation if necessary.

Appendix 1

Access Request

At Hale Prep School, procedures for responding to subject access requests comply with current legislation, GDPR.

There are two distinct rights of access to information schools hold about pupils. Individuals have the right to request access to the personal information held about them.

These procedures relate to subject access requests made under current legislation.

Making a subject access request:-

Requests for information must be made in writing - which includes email - and be addressed to the headmaster. Further enquiries will be made if the initial request needs to identify the required information.

The requestor's identity must be established and clarified before disclosing any information, and checks should also be carried out regarding proof of relationship to the child. Parents/guardians.

Once officially received, the response time for subject access requests is one month.

The GDPR allows exemptions to provide some information; therefore, all information will be reviewed before disclosure.

Third-party information has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third-party information, consent should normally be obtained from the third party. There is still a need to adhere to the 1-month statutory timescale. If a request pertains to information provided by a 3rd party, i.e., Consent must be obtained before disclosure.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse or information relating to court proceedings.

If there are concerns over the disclosure of information, then additional advice should be sought. Where redaction (information blacked out/removed) has taken place, a full copy of

the information provided should be retained to establish if a complaint is made, what was redacted, and why. The information disclosed should be clear. Thus any codes or technical terms will need to be clarified and explained. If the information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Information can be provided at the school with a staff member to help and explain matters if requested or provided face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery.
If postal systems have to be used, registered/recorded mail must be used.

Complaints
Complaints about the above procedures should be made to the headteacher.
Complaints that are inappropriate to be dealt with through the school's complaint procedure can be handled by the Information Commissioner.
Appendix 2
Information security roles

Overall responsibility for Safeguarding rests with the Senior Management Team; some key roles exist in delivering the Safeguarding agenda. It is important that appropriate individuals within schools are identified and that they fully understand their roles and their associated responsibilities in delivering the roles' core objectives.

Data Protection Administrator
The Data Protection Administrator is Mrs Ruth Vayro. She has the following responsibilities:

- To review and update this policy
- To be clear about what data the school holds, how long it is stored and how it is deleted.
- To be clear, who has access to the data

Computers
Mrs Taylor is the IT Co-ordinator. Dan Jones has responsibility for managing the network, monitoring its performance and security.

Appendix 3

Data security guidance

What is sensitive or personal information?

Much information you can access within schools will be classed as publicly available. This information is not sensitive or personal and would not cause anyone or the organisation any harm or embarrassment. However, if the information includes sensitive or personal details, this information needs to be handled and protected by the school's data security policy.

Information of this nature can be in physical (printed out) or electronic format. Information in electronic format can have access controls applied to it. Still, these logical controls are only useful if the end-user prints this information out and leaves it on the printer in a public area of the school. This information could be situated within individual word-processing, spreadsheet or database files or entered into the school's information management system or any other centralised system the school may be using.

Listed below are the types of information that can be categorised as sensitive or personal.

Sensitive

Sensitive information covers any information you might not want to be made publicly available as it could potentially cause embarrassment or damage your reputation.

- Staff absence records
- Staff contract and pay details
- Contact and next of kin details
- Disability and medical issues

- Pupil special educational needs details
- Pupil assessment data and reports
- Pupil in care or child protection register details
- Ethnicity
- Sexuality

Appendix 4

Complying with the GDPR

Allowing individuals to see their information

Pupils, their parents or carers and staff have the right to see the personal information schools hold about them and to correct the information if it is wrong. Under the GDPR, they can send a subject access request to the school. They can also request the right to become invisible and be removed from the school's records. If this were to happen, the school would keep a copy of the request for proof.

Notifying the Information Commissioner's Office

All schools must notify the Information Commissioner's Office (ICO) that they handle personal information. Notification is statutory, and failure to do so is a criminal offence.

Appendix 5

BREECH

If a breach occurs, it will be reported to Mrs Vayro. In line with the GDPR, if there were a risk to the individual, she would inform the ICO of the breach within 72 hours of knowing; the individual would only be informed if there was a 'high risk'. The Senior Management Team would carry out the risk assessment. External advice would be sought if deemed necessary.

Appendix 6

ACCESS TO PERSONAL DATA REQUEST – SUBJECT ACCESS REQUEST

Subject's Surname: ……Subject's Forenames: ……

Subject's Address: ……

……

Postcode: …… Telephone Number: ……

Are you the person who is the subject of the records you are enquiring about? YES / NO (i.e. the "Data Subject")? If NO, Do you have parental responsibility for a child who is the "Data Subject" of records you are enquiring about?

YES / NO If YES, the Name of the child or children about whose personal data records you are enquiring

……

Description of Concern / Area of Concern

……

Description of Information or Topic(s) Requested (In your own words) DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under the GDPR and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School. I agree that the reply period will commence when I have supplied sufficient information to enable the School to

perform the search. I consent to the reply being disclosed and sent to me at the address above.

Signature of "Data Subject" (or Subject's Parent):

……

Name of "Data Subject" (or Subject's Parent): ……

PRINTED) Date: ……