

Data Protection and Data Security Policy

Aligned with Ofsted, NCFE, SEND Code of Practice, Equality Act, and KCSIE



This is a controlled document and, as such, will be kept read only. Any changes must be approved by the Author.

Author	Version No	Date Approved	Review Date
Adam Smyth	V1.0	November 2024	November 2025
Adam Smyth	V1.1	September 2025	September 2026

Table of Contents

1. Introduction	3
2. Policy Objectives	3
3. Scope	3
4. Key Principles	3
5. Roles and Responsibilities	4
5.1 Data Controller	4
5.2 Education Business Manager (Data Protection Officer)	4
5.3 All Staff	4
6. Data Collection and Processing	4
6.1 Types of Data Collected	4
6.2 Sensitive Data	4
6.3 Data Use	4
7. Safeguarding and SEND Considerations	5
7.1 Safeguarding Data:	5
7.2 SEND Support:	5
8. Data Security Measures	5
8.1 Access Control	5
8.2 Secure Storage	5
8.3 Data Breaches	5
8.4 Data Subject Rights	5
9. Retention and Disposal	6
9.1 Retention Periods	6
9.2 Disposal	6
10. Monitoring and Review	6
11. Communication and Training	6

DATA PROTECTION AND DATA SECURITY POLICY

1. INTRODUCTION

Hatfield Wick Education (HWE) is committed to processing and protecting personal data in compliance with the **UK General Data Protection Regulation (UK GDPR)**, **Data Protection Act 2018**, and other applicable laws. This policy ensures that personal data is handled lawfully, fairly, transparently, and securely. It also reflects safeguarding responsibilities under Keeping Children Safe in Education (**KCSIE**) and considerations for learners with special educational needs and disabilities (SEND) under the **SEND Code of Practice**.

2. POLICY OBJECTIVES

This policy aims to:

- 2.1 Ensure all personal data is processed lawfully, fairly, and transparently.
- 2.2 Safeguard sensitive information, particularly safeguarding and SEND-related data.
- 2.3 Comply with regulatory and inspection requirements, including those of Ofsted and awarding organisations such as NCFE.
- 2.4 Clarify roles and responsibilities for data protection and data security across HWE.

3. SCOPE

This policy applies to all personal data processed by HWE, whether held electronically or in physical records. It covers learners, staff, contractors, parents/carers, and other stakeholders.

4. KEY PRINCIPLES

HWE adheres to the following data protection principles:

- 4.1 **Lawfulness, Fairness, and Transparency:** Data is processed only where lawful grounds exist, and individuals are informed about how their data is used.
- 4.2 **Purpose Limitation:** Personal data is collected for specified, legitimate purposes and not processed for unrelated reasons.
- 4.3 **Data Minimisation:** Only the data necessary for processing purposes is collected.
- 4.4 **Accuracy:** Reasonable efforts are made to ensure data is accurate and up to date.
- 4.5 **Storage Limitation:** Personal data is retained only for as long as necessary.
- 4.6 **Security:** Appropriate technical and organisational measures are implemented to safeguard data.
- 4.7 **Accountability:** Hatfield Wick Education takes responsibility for, and is able to demonstrate, compliance with these principles.

5. ROLES AND RESPONSIBILITIES

Data Controller

Hatfield Wick Education acts as the data controller, determining the purposes and means of processing personal data.

Education Business Manager (Data Protection Officer)

- Oversees compliance with data protection laws.
- Acts as the main contact for data protection queries and requests.
- Provides training and updates on data protection responsibilities.
- Coordinates data breach responses.

All Staff

- Handle personal data in line with this policy and relevant laws.
- Report data breaches immediately to the Data Protection Officer.
- Ensure personal data is stored securely and accessed only for authorised purposes.

6. DATA COLLECTION AND PROCESSING

Types of Data Collected

HWE collects and processes:

- Personal identifiers (e.g., names, address, contact details).
- Academic records, attendance, progress and assessment data.
- Medical, SEND, and wellbeing information (where applicable).
- Safeguarding records, as required under **KCSIE**.

Sensitive Data

Special category data is processed only where a lawful basis applies, including legal obligation, public task, or vital interests.

Consent will not be relied upon where safeguarding or statutory duties apply.

Data Use

Data is used for:

- Managing enrolment and academic progress.

- Safeguarding learners and supporting SEND needs.
- Compliance with NCFE and other awarding organisations, regulatory, and inspection requirements.

7. SAFEGUARDING AND SEND CONSIDERATIONS

Safeguarding Data:

- Data related to safeguarding is managed confidentially and shared only on a need-to-know basis in line with **KCSIE**.
- Safeguarding data may be shared without consent where required to protect a child or meet statutory obligations.

SEND Support:

- Data on learners with SEND is processed to provide appropriate support and adjustments.
- SEND data is shared only when necessary for the learner's educational outcomes.

8. DATA SECURITY MEASURES

Access Control

- 8.1.1 Data access is restricted to authorised individuals.
- 8.1.2 Strong passwords and two-factor authentication are used for digital systems.

Secure Storage

- 8.1.3 Physical records are stored in locked cabinets.
- 8.1.4 Digital data is encrypted and regularly backed up.

Data Breaches

- 8.1.5 All breaches are reported to the Data Protection Officer immediately.
- 8.1.6 Significant breaches are reported to the **Information Commissioner's Office (ICO)** within **72 hours**.
- 8.1.7 Affected individuals will be informed where there is a high risk to their rights and freedoms.

Data Subject Rights

Individuals have the right to:

- 8.1.8 **Access:** Request access to their personal data.
- 8.1.9 **Rectification:** Correct inaccurate or incomplete data.

8.1.10 **Erasure:** Request deletion of data, subject to legal or safeguarding obligations.

8.1.11 **Restriction:** Limit processing of their data in certain circumstances.

8.1.12 **Objection:** Object to data processing where lawful grounds exist.

9. RETENTION AND DISPOSAL

Retention Periods

Data is retained only as long as necessary for legal or operational purposes. For example:

- Safeguarding records: Retained in accordance with **KCSIE** guidelines.
- Academic records: Retained for regulatory purposes (e.g., NCFE audits).

Disposal

- Physical records are shredded when no longer required.
- Digital data is permanently deleted using secure methods.

10. MONITORING AND REVIEW

10.1.1 **Policy Review:** The Data Protection Policy is reviewed annually to ensure ongoing compliance with UK GDPR, **Ofsted**, and **NCFE** requirements.

10.1.2 **Audits:** Regular audits assess the effectiveness of data security measures and compliance with this policy.

11. COMMUNICATION AND TRAINING

11.1.1 **Staff Training:** All staff receive data protection training during induction and regular updates thereafter.

11.1.2 **Learner Awareness:** Data protection practices are explained during enrolment and made accessible via the HWE website.

This policy ensures the lawful, secure, and fair processing of personal data, safeguarding the rights and welfare of all stakeholders.