Data Protection Policy

General Data Protection Regulation (GDPR)

Henry David Learning

Woodfield School

August 2026 – August 2027

Agreed by the Proprietor:	August 2024
Review date:	August 2025
Review date:	August 2026
Updated by Deb Wilson	August 2026
Review date:	August 2027

The purpose of this policy is to assist Woodfield School to meet its legal obligations under the 1998 Act. It describes the duties of everyone working at Woodfield School and the rights of access by individuals to their personal data. This policy also sets out the eight data protection principles which Woodfield School must comply with when processing personal data.

Definition of key terms: General Data Protection Regulation (GDPR)

Data Controller
Like the existing Data Protection Act (DPA), the GDPR applies to Data Controllers who process personal data. So first, who is the Data Controller? This is a person who decides the purpose for which any personal data is to be processed and the way in which it is to be processed. This can be decided by one person alone or jointly with other people.

Data Processor

Unlike the DPA, the GDPR introduces specific responsibilities for the Data Processor. These are third parties that process data on behalf of the Data Controller and includes IT service providers. An employee of a company which decides what and how personal data is to be processed is a Data Controller, not a Data Processor.

Personal Data
The GDPR has a broader definition of what constitutes personal data than the DPA, by incorporating reference to identifiers such as name, identification numbers, IP address and location. Each person to which the personal data refers is known as a Data Subject.

Sensitive Personal Data
The GDPR definition of sensitive personal data is slightly broader than under the DPA. The main addition is biometric data, for the purposes of uniquely identifying a person. The GDPR talks about a special category of personal data rather than sensitive personal data but the definition is almost the same. The table below illustrates what is sensitive and what isn't, and what isn't personal data.

Right to be forgotten
The right to erasure of personal data or 'the right to be forgotten' enables an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

Data Protection Officer

A Data Protection Officer is someone who is given formal responsibility for data protection compliance within a business. Not every business will need to appoint a data protection officer – you need to do so if:

- Your organisation is a public authority;
- You carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Data Protection Authority
The Data Protection Authority in the UK will still be the UK Information Commissioner, who is tasked by the EU with the monitoring and enforcement of the GDPR within the UK. The UK will implement GDPR so that it continues to be in force after Brexit takes effect.

Privacy Impact Assessments
A Privacy Impact Assessment (PIA) is an obligatory method of identifying and reducing privacy risks to individuals through the misuse of their personal information when you are undertaking new projects handling personal data.

Profiling
Profiling means automated processing of personal data for evaluation analysis or prediction. When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

Scope:

The policy applies equally to all employees at Henry David Learning, Woodfield School.

Principles
The eight principles set out in the 1998 Act require Personal Data to be:
1: Processed fairly and lawfully
2: Obtained for a specified and lawful purpose
3: Adequate, relevant and not excessive in relation to the purpose for which it is processed
4: Accurate and up to date
5: Kept for no longer than is necessary for the purpose for which it is processed
6: Processed in accordance with the data subject's rights
7: Protected against unauthorised or unlawful processing, loss or damage through appropriate technical and organisational measures
8: Prevented from being transferred to a country or territory outside the European Economic Area unless that country has an adequate level of protection.

Data subject rights: The GDPR endows individuals with eight data subject rights.

The right to be informed
Organisations need to tell individuals what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.

The right of access
Individuals can submit subject access requests, which oblige organisations to provide a copy of any personal data they hold concerning the individual. Organisations have one month to produce this information, although there are exceptions for requests that are manifestly unfounded, repetitive or excessive.

The right to rectification

If an individual discovers that the information an organisation holds on them is inaccurate or incomplete, they can request that it be updated. As with the right of access, organisations have one month to do this, and the same exceptions apply.

The right to erasure
Individuals can request that organisations erase their data in certain circumstances, such as when the data is no longer necessary, the data was unlawfully processed or it no longer meets the lawful ground for which it was collected. This includes instances where the individual withdraws consent.

The right to erasure is also known as 'the right to be forgotten'.

The right to restrict processing
Individuals can request that an organisation limits the way it uses personal data. It's an alternative to requesting the erasure of data, and might be used when an individual contests the accuracy of their personal data or when they no longer need the information but the organisation requires it to establish, exercise or defend a legal claim.

The right to data portability

Individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent.

The right to object
Individuals can object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority. Organisations must stop processing information unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual or if the processing is for the establishment or exercise of defence of legal claims.

Rights related to automated decision-making including profiling

The GDPR includes provisions for decisions made with no human involvement, such as profiling, which uses personal data to make calculated assumptions about individuals. There are strict rules about this kind of processing, and individuals are permitted to challenge and request a review of the processing if they believe the rules aren't being followed.

Duties
To meet legal obligations, you must:

- Check that any Personal Data obtained is necessary for the purpose of fulfilling Woodfield School's duties
- Understand why Personal Data is being collected and be able to communicate that to relevant persons
- Only use Personal Data for the purpose for which it was obtained
- Ensure that Personal Data is held securely, whether on paper or electronically. Personal Data should not be removed from Woodfield School's premises, wherever possible
- Check that any Personal Data that you process for Woodfield School is accurate and up to date
- Notify Woodfield School of any changes to your Personal Data such as address and telephone numbers
- Check that Personal Data held is still required; and delete Personal Data when it is no longer needed (see Retention of Personal Data below).
-

Retention of Personal Data

- You should regularly review whether Personal Data that you process should be retained or deleted. Some Personal Data will need to be held for longer periods than others. For example, a report in relation to a Serious Untoward Incident (which may include the names of pupils or members of staff) should be held for a limited period of time, whereas documents (which may include the names and CVs) should be held for six years from the date. In each case, you should consider the subject matter and the purpose for which it is processed.

- Woodfield School has a disposal and retention schedule which sets out the types of records that we hold, how long they must be kept for and how they must be eventually disposed of.

Consequences of breach

The Information Commissioner is responsible for enforcing the 1998 Act. He has the power to:

- Conduct assessments to check organisations are complying with the 1998 Act
- Serve information notices requiring organisations to provide specified information
- Serve enforcement notices and “stop now” orders where there has been a breach of the 1998 Act
- Prosecute those who commit criminal offences under the 1998 Act
- Conduct audits to assess whether organisations processing of Personal Data follows good practice
- Report to Parliament on data protection issues of concern.

You must not:

- Wilfully destroy information a person is entitled to access under the 1998 Act; or
- Unlawfully obtain or disclose Personal Data.

These actions may result in a fine or term of imprisonment.

Right to access information

All individuals who are the subject of Personal Data held by Woodfield School are entitled to:

- A description of the data held about them and of why it is being held
- A copy of the Personal Data held on them together with the source
- Information on what Woodfield School is doing to comply with its obligations under the 1998 Act; and keep their Personal Data up to date.

Woodfield School may charge an appropriate fee for providing a copy of Personal Data. The maximum fee charge is set out in the 1998 Act and is £10 at the date of this policy.
In some circumstances, Woodfield School may withhold information. The bases upon which it may withhold information are set out in the 1998 Act.

Any person who wishes to exercise this right should make a request in writing to HR who can be contacted at hr@henrydavidlearning.co.uk Appendix 1 Subject Access Request

Woodfield School aims to respond to requests for access to Personal Data as quickly as possible, but in any event will ensure that it responds within the prescribed period which is 40 days from receipt of a written request. If there is delay, Woodfield School will provide reasons in writing to the individual making the request.
If personal details are inaccurate, they can be amended upon request.

Appendix 1

Subject Access Request Form

Henry David Learning

1. Overview

1.1 The UK General Data Protection Regulations (UK GDPR) provides you, the data subject, or someone you authorise on your behalf, with a right to request a copy of the data/information we hold about you.

1.2 This request is known as a subject access request. In order to initiate a subject access request please complete the following form and return it to us along with proof of your identity for verification purpose. Once your identity has been checked the copy of your ID will be destroyed.

1.3 If you are acting on behalf of someone else you will need to provide proof of your identity along with proof of authority to act on behalf of the data subject.

1.4 Once you submit a subject access request to Henry David Learning, we will verify the information that you have submitted and will then respond to you within one calendar month.

2. Requesting Information

2.1 The completed form and all accompanying documents should be sent to hr@henrydavidlearning.co.uk

Henry David Learning Ltd
First Avenue
Centrum 100
Burton-On-Trent
DE14 2WE

3. Paying for Information

3.1 Please note: there are no set fees for subject access requests. However, if Henry David Learning deems it to be excessive or manifestly unfounded, there will be a reasonable fee to cover the administrative costs of complying with the request or the request may be refused. There is also an ability to charge a reasonable fee if an individual requests further copies of data.

Appendix A - Subject Access Request (SAR) Form

Woodfield School

Under UK GDPR, individuals have the right to request access to personal data held about them. Complete this form to help the school process your request.

Section 1: Requester Details

Full name:

_____

Address:

_____

Telephone number:

_____

Email address:

_____

Section 2: Who is the Request About?

☐ Myself ☐ My child ☐ Another individual

_____

Name of individual:

_____

Relationship to individual:

_____

Section 3: Information Requested

Describe the information requested:

_____

Dates/date range (if known):

_____

Relevant staff, departments or record types:

_____

Section 4: Preferred Format

☐ Electronic copy by secure email

_____

☐ Paper copy

_____

☐ Inspection of records (where appropriate)

_____

Section 5: Identity Verification

Attach proof of identity where requested.

_____

☐ Passport ☐ Driving Licence ☐ Utility Bill ☐ Other

_____

Section 6: Declaration

I confirm that the information provided is accurate and that I am entitled to request this information.

Signature: _____

Date: _____

School Use Only

Date received: _____

Identity verified: _____

Reference number: _____

Response due by: _____

Officer handling request: _____

Outcome: _____