Hay-on-Wye CP School

Data Protection Policy (Schools)

Signed: Chair of Governors	Date: 18.12.23 ratified 19.01.24 Signed.
Signed: Headteacher	Date: 18.12.23 19.01.24
Date of Review:	December 2023

Policy Document Control:

Organisation	Hay on Wye CP School
Title	Data Protection Policy
Author	Professional Lead - Data Protection
Owner	Hay on Wye CP School
Subject	Schools Information Governance (IG) Policy
Protective Marking	No protective marking
Version	2
Review Date	Autumn 2025

Revision History:

Revision Date	Summary of Change	Contact	Review Date
2022	Re-draft: - Multiple amendments - Multiple additional information - Policy Document Control	Information Compliance	
December 2023	Adopted to replace the previous policy version	Hay on Wye CP School Policy Committee	Autumn 2025

Policy Contents:

1. Definitions:

1.1. *UK General Data Protection Regulations ('UK GDPR')/Data Protection Act 2018 ('DPA 2018')* – In effect, these are regulations that lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

1.2. *Personal Data* – Any information relating to an identified or identifiable natural person ('data subject'); [directly or indirectly identified], in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.3. *Special Category data* – Personal data that is of a more sensitive nature, such as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

1.4. *Controller* – The body which, alone or jointly with other bodies, determines the purposes and means of the processing of personal data.

1.5. *Processor* – The body which processes personal data on behalf of the controller.

1.6. *Third Party* – A body other than the data subject, controller and processor who, under direct authority of the controller or processor, are authorised to process personal data.

1.7. *Processing* – Covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, erasure, or destruction of personal data.

1.8. Data Protection Officer (DPO) – An individual appointed by the controller to assist them monitor internal compliance, inform and advise of a controller's data protection obligations, provide independent advice regarding Data Protection Impact Assessments and act as a contact point for data

subjects and the Information Commissioner's Office. DPO (Schools) information.compliance@powys.gov.uk

2. Policy Introduction & Statement:

2.1. The School processes personal data about staff, pupils, parents, and other individuals who come into contact with the school in order to provide education and other associated functions.

2.2. As a controller, the School must ensure that its processing of personal data complies with data protection legislation such as the UK GDPR and the DPA 2018.

3. Policy Purpose:

3.1. This policy is intended to ensure that personal data is managed correctly and securely in accordance with data protection legislation, as well as other related legislation that may need to be considered when processing personal data, such as the Human Rights Act 1998.

3.2. This policy will outline how the School will manage:
3.2.1. risks associated to the processing of personal data;
3.2.2. data protection rights requests;
3.2.3. personal data breaches.

3.3. Where relevant, this policy will sign post the reader to any related documentation.

3.4. It will hold the School and school staff accountable to their responsibilities to personal data, and will ensure that personal data, including special category personal data, is processed in line with the 7 principles that are set out in Article 5 of the UK GDPR.

3.5. The consequences of failing to comply with data protection legislation can lead to personal data breaches, increased data protection complaints, loss of public confidence, reputational damage including embarrassment and, in some cases, regulatory action from the Information Commissioners Office (ICO) including fines.

4. Scope:

4.1. This policy applies to all School staff, contractual third parties or other individuals who may process any personal data to which the School is controller of.

4.2. All users must understand and adopt the use of this policy when handling personal data.

5. **Responsibilities**:

5.1. The Head Teacher and Chair of Governors have overall responsibility for ensuring the School's compliance with this policy and with data protection legislation.

5.2. Each Senior Leader is responsible for:

5.2.1. ensuring that all systems, processes, records and datasets within their area are compliant with this policy and with data protection legislation;
5.2.2. assisting the DPO with their data protection duties by providing all information upon request and additional support where necessary;
5.2.3. ensuring that their staff are aware of their data protection responsibilities;
5.2.4. consulting the DPO on issues affecting the use of personal data or any new project that introduces additional processes to personal data;
5.2.5. ensuring that Data Protection Impact Assessments (DPIAs) are undertaken as appropriate on data processing activities within their area (in consultation with the DPO).
5.2.6. ensuring that the data protection rights of the individual are respected.

5.3. The DPO shall provide advice and assistance on the data protection matters outlined within this policy but is not responsible for the Schools compliance with this policy or data protection legislation.

6. Data Protection Principles:

6.1. The School is responsible for ensuring compliance with the principles of processing personal data that are set out in Article 5 of the UK GDPR.

6.2. There are 7 Principles:

6.2.1. [**1st Principle – Lawful, fair and transparent**] Processed lawfully, fairly and in a transparent manner in relation to the data subject.
6.2.2. [**2nd Principle – Purpose limitation**] Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
6.2.3. [**3rd Principle – Data minimisation**] Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
6.2.4. [**4th Principle - Accuracy**] 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.
6.2.5. [**5th Principle – Storage limitation**] 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.
6.2.6. [**6th Principle – Integrity and confidentiality**] 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 organisational measures.

6.2.7. The School shall be responsible for, and be able to demonstrate compliance with, all of the above, otherwise known as the "Accountability principle" which is the **7th principle**.

7. Data Protection Rights

7.1. The UK GDPR sets out 9 rights that data subjects have in respect of the processing of their personal data.

7.2. The School will ensure that an individual's rights over their personal data are respected, and all requests to exercise such rights are actioned appropriately.

7.3. These rights include:

7.3.1. [**Article 13 & 14**] The right to be informed that processing is being undertaken. The School will ensure privacy notices are accessible to data subjects whose personal data is being processed, including pupils, parents and School employees.

7.3.2. [**Article 15**] The right of access to a data subjects own personal data and to specific information about the processing.

7.3.3. [**Article 21**] The right to object to and prevent processing in certain circumstances.

7.3.4. [**Articles 16 & 18**] The right to rectify or restrict processing of inaccurate data.

7.3.5. [**Article 17**] The right to erasure in certain circumstance.

7.3.6. [**Article 20**] The right to data portability in some limited circumstances.

7.3.7. [**Article 22**] The right to have human input in decisions based solely on automated processing.

7.4. All requests made by individuals relating to their personal data rights will be referred to the Headteacher and undertaken in consultation with the DPO. The School must ensure that appropriate action is taken and a response is issued without delay and at least within one calendar month.

7.5. This policy supports the Schools Request Procedure (UK GDPR, FOI & EIR).

8. Data Protection by Design & Default:

8.1. The School will apply a 'data protection by design and default' approach to the processing of personal data. This means that the School will assess the risks of processing personal data before implementing a new system or project and will agree appropriate mitigation measures to those risks.

8.2. The School will conduct and will be responsible for completing a Data Protection Impact Assessment ('DPIA') with any introduction of systems or processing that may result in a high-risk impact to the rights or freedoms of data subjects.

8.3. The School will consult with the DPO on all DPIAs undertaken who will provide the School with advice and recommendations on the completed assessment. The DPO will not be responsible for completing the DPIA.

8.4. This policy supports the Data Protection Impact Assessment Policy.

9. Personal Data Breaches:

9.1. Any personal data breach (or information security incident) that impacts upon the confidentiality, integrity or availability of personal data held by the School must be reported immediately to the Schools DPO who will assist the School to action and respond to it accordingly.

9.2. This may include but is not limited to, incidents such as:

9.2.1. The loss of records, laptops or media containing personal data;

9.2.2. Unauthorised access to information systems containing personal data;

9.2.3. Access to personal data with no identified business need;

9.2.4. Personal data being misdirected to the incorrect recipient;

9.2.5. Loss of access to systems containing personal data.

9.3. All reported incidents will be recorded to ensure an investigation is undertaken to establish reasons for the incident, and ascertain the impact upon data subject(s) and School, identify improvements or lessons learnt, and ensure the appropriate mitigation measures are put in place and adhered to.

9.4. The DPO, in liaison with the School, will consider, where the incident is of sufficient severity or poses a risk to the individual, whether to report the personal data breach to the Information Commissioners Office (ICO). Where the DPO determines that an incident constitutes a reportable data breach, then they will report the incident to the ICO and liaise as appropriate.

9.5. If the data breach constitutes a high risk to the data subject, then the School will also inform those data subject(s) affected of the risk and potential impact on them.

9.6. This policy supports the Personal Data Breach Policy.

10. Complaints:

10.1. The School will manage a complaint made by a or on behalf of a data subject in compliance with the School's complaints policy. Complaints made in regard of the Schools management of personal data will be discussed with the DPO who will advise the School accordingly.

11. Contacts:

11.1. If you have any enquires in relation to this policy, please contact Mr Richard Morris, Headteacher who will also act as the contact point for any Subject Access Request (SAR).

11.2. Further advice and information is available from the Information Commissioner's Office, Home / ICO or telephone 0303 123 1113 or 029 2044 8400 for the Wales Regional Office.

12. Review:

12.1. This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the DPO, Headteacher, or nominated representative.