DATA PROTECTION POLICY

This section should be completed following ratification of the Policy.

Audience	Trust Leaders, Trustees, All Staff, Parents, Contractors and other interested parties
Ratified	February 2026
Other Related Policies	Privacy Notices, Child Protection and Safeguarding Policy, Cybersecurity Policy
Policy Owner	ARC Committee
Review Frequency	Annually

Ownership
Preston Hedges Trust is responsible for the production and maintenance of this document. It is issued by the Clerk, clerk@prestonhedges.org to whom any change requests or queries should be directed.

Contents

Statement of Intent

1	Legislation and Guidance
2	Definitions
3	Roles and Responsibilities
4	Data Protection Principles
5	Consent
6	Processing Data
7	Individual Rights
8	Sharing Personal Data
9	Subject Access Requests
10	Photographs and Videos
11	CCTV
12	Use of Generative Artificial Intelligence (AI)
13	Data Protection by Design
14	Data Security and Storage of Records
15	Disposal of Records
16	Data Breaches
17	Publication of Information
18	Training
19	Monitoring arrangements

Statement of intent

Preston Hedges Trust is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller, ensuring the handling of such data is in line with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act.

This policy is in place to ensure all staff and Trustees are aware of their responsibilities and outlines how the Trust and its schools comply with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

In this policy, "the Trust" refers to Preston Hedges Trust as the data controller for all personal data processed across the organisation. "Schools" refers to the individual academies within the Trust, which act on behalf of the Trust when collecting, storing and using personal data in accordance with this policy.

1. Legislation and Guidance

The UK General Data Protection Regulation (UK GDPR) is a UK law that took effect on 01 January 2021 and sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679), which was applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The DPA 2018 sets out the framework for data protection law in the UK. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

The DUAA is a new Act of Parliament that updates some laws about digital information matters. Due to the Data (Use and Access) Act coming into law on 19 June 2025, It changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights. Changes will be phased in between June 2025 and June 2026.

ICO guidance is under review and may be subject to change. This Policy will be updated following changes to Guidance when provided by the ICO.

This Policy reflects relevant changes:

New 'recognised legitimate interests' lawful basis: when the school uses personal information for certain 'recognised legitimate interests', DUAA removes the need for the school to balance the impact on the people whose personal information we use, against the benefits arising from that use. For example, when protecting public security.

Disclosures that help other organisations perform their public tasks: it allows the school to give personal information to organisations such as the police, without having to decide whether the school needs the

information to perform our public tasks or functions. Instead, the organisation making the request is responsible for this decision.

Assumption of compatibility: it allows the school to assume that some re-uses of personal information are compatible with the original purpose you collected it for, without having to do a compatibility test. This includes disclosing personal information for the purposes of archiving in the public interest, even if you originally only got consent for a different purpose.

Subject access requests (SARs): it makes it clear that the school only has to make reasonable and proportionate searches when someone asks for access to their personal information.

Data protection legislation shall be monitored and implemented to remain compliant with all requirements.

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

2. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf.

3.1. Data Controller

The Trust processes personal data relating to parents and carers, pupils, staff, Trustees, visitors and others, and therefore is a data controller. The Trust is registered with the ICO, as legally required.

3.2. Trust Board

The trust board has overall responsibility for ensuring that the trust and its schools complies with all relevant data protection obligations.

3.3. Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and acts as a contact point for data subject requests and the supervisory authority.

They will conduct data protection audits, providing a written report to the audit, risk and compliance committee on their advice and recommendations on areas of improvement relating to data protection issues.

The Data Protection Officer (DPO) is Ruth Hawker, Plumsun Ltd. Contact details can be found on the website: www.plumsun.com

The DPO is independent, an expert in data protection, adequately resourced, and reports to the highest management level.

3.4. Principal

The Principal acts as the representative of the data controller on a day-to-day basis, supported by the Chief Operating Officer (COO) for the Trust.

3.5. All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Principal / COO or DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

4. Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

5. Consent

When we rely on consent as the legal basis for processing personal data (as defined in Article 6 and Article 9 of the UK GDPR), we ensure that the following standards are strictly met:

- Voluntary and Specific: Consent must be a freely given indication of the individual's wishes, without coercion, and must relate to specific, identified processing purposes.
- Informed: The data subject will be fully informed regarding the nature and extent of the processing, including the types of data involved and the purpose of processing, prior to granting consent.
- Unambiguous Indication: Consent must be provided by a clear, affirmative action. It shall not be inferred from silence, inactivity, or the use of pre-ticked boxes.
- Withdrawal of Consent: The individual retains the right to withdraw consent at any time. The process for withdrawal will be as straightforward as the process for granting consent.

5.1. Documentation of Consent

We maintain an auditable record documenting precisely how and when consent was obtained, along with the information provided to the data subject at that time.

6. Processing Data

Processing is necessary for the performance of a task carried out in the *public interest* or in the exercise of official authority vested in the controller. The Trust will only process personal data where it has 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

6.1. Special Category Data

Special Category Data is personal data (as defined in the relevant section of Article 9) that's considered more sensitive and given greater protection in law. The Trust or school processes special category data, which is directly linked to the school's lawfulness of processing, tasks carried out in the public interest, and specifically, paragraphs 6 to 28 of schedule 1 of the Data Protection Act 2018;

- Equality of opportunity or treatment
- Safeguarding of children and of individuals at risk
- Preventing fraud

Special category data the school includes:

- racial or ethnic origin
- religious or philosophical beliefs
- trade-union membership
- biometric information (for example, a fingerprint)
- health matters (for example, medical information)
- sexual matters or sexual orientation

The school includes, as 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)

If personal information meets the above criteria, then individuals who have personal information held by us will be made aware of the personal information and the criteria for holding the information and the length of time is the information is held is in the 'Information Audit' and 'Retention' document, located on our website.

7. Individual Rights

Individuals have the right to:

- Be informed about what data is being held.
- Be informed about how and why the data is being processed.
- The right to access any data that is being held.
- The right to request that any data is erased.
- The right to restrict processing.
- The right to data portability (that the individual can transport the data held about them to another service) if the data is held by automatic means.
- The right to object to the way data is being held or processed.
- The right not to be subject to automated decision-making. The individual can write to the Principal or COO regarding requests for data to be erased, to restrict processing, to data portability, to not be subject to automated decision-making, or the right to object to the way data is being held or processed.
- Where personal data is no longer required for its original purpose, an individual can request that the processing is stopped and all their personal data is erased by the Trust or school including any data held by contracted processors.

8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject Access Request

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the school or Trust holds about them. A child has the right to make a subject access request for themselves, specified under UK GDPR guidance. Further guidance can be sort via the ICO website

A subject access request should be made in writing to the Principal. The request should ideally include the following:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

The Trust shall respond to reasonable and proportionate requests within one month, unless it is a complex request. Where a request is complex or numerous the Trust will inform the individual within 1 month that it will comply within 3 months of receipt of the request, providing an explanation as to why the extension is necessary

In line with our safeguarding and UK GDPR obligations, some personal information may be redacted for reasons such as:

- Information that might cause serious harm to the physical or mental health of the pupil or another person; • Information requested that would not be in the best interest of the child
- Information containing personal information about more than one individual. The Data Protection Officer will independently advise any requests as necessary. They will act as a contact point for data subjects and the supervisory authority.

The Trust or school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.

10. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent and the pupil.

Any photographs and videos taken by parents at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within the school on display boards, in newsletters or curriculum books, etc.
- Use by the Trust in brochures, newsletters, other promotional materials, etc.
- Use by external agencies such as the school photographer or newspapers
- Online on our school and Trust websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the COO via clerk@prestonhedges.org.

12. Use of Generative Artificial Intelligence (AI)

The Trust recognises that generative AI technologies involve the processing of extensive datasets and may pose increased risks to data privacy and security.

Staff and pupils must not input personal, identifiable, or sensitive data into generative AI platforms unless the system has been formally assessed, and explicit approval has been granted following a full DPIA.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in the Trust and its schools operations.

Use of generative AI tools must comply with the Trust's Acceptable Use Policy. Individuals must not rely solely on AI-generated outputs without appropriate human oversight and validation.

Any incidents, breaches, or concerns arising from the use of AI tools must be reported immediately to the COO and DPO and will be investigated in line with the Trust's data breach procedures.

13. Data Protection by Design

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.

- Completing data protection impact assessments where the Trust or school's processing of personal data presents a high risk to rights, and when introducing new technologies (advice to be sought from the DPO if required).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14. Data Security and Storage of Records

The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

The following guideline are in place for staff in order to minimise the risk of personal data being compromised:

- Paper-based records or personal information are out of site and kept under lock and key when not in use
- Paper-based records or personal information should not be taken off site, unless permission has been granted by the Principal (such as the need for emergency information during educational visits). The information should be stored securely and not be on view in public places, or left unattended under any circumstances.
- Unwanted copies of personal or sensitive information should be shredded, this includes notes from a meeting that contains a pupils or staff members name.
- Staff members should use their Print ID's to access print materials to avoid personal or sensitive information being left on the printers.
- Staff members should ensure their PC's or laptops are locked or shut down before leaving their device unattended. A privacy screen should be utilised if working in an area where other staff members, pupils or visitors could see sensitive information on the screen.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely.

The Trust will shred or incinerate paper-based records, and overwrite or delete electronic files. The Trust also use a third party to safely dispose of records on the Trust and school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and request confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance.

16. Data Breaches

- Internal Reporting
  - Any suspected breach must be immediately reported to the Principal or COO.
  - Report must include details on the nature of the breach, affected data, and individuals, if known.
- Assessment and ICO Reporting
  - The Principal/COO will promptly assess the risk to individuals' rights and freedoms.
  - The Principal/COO must report the breach to the ICO within 72 hours of becoming aware, UNLESS the breach is unlikely to result in a risk to individuals.
  - All breaches, regardless of external reporting, must be documented internally and will reported to the audit, risk and compliance committee.
- Individual Notification
  - Affected individuals must be notified without undue delay if the breach is likely to result in a HIGH risk to their rights and freedoms.
- DPO and Remedial Action
  - The Data Protection Officer (DPO) must be immediately informed and providing expert advice on assessment, reporting, and compliance.
  - Immediate action is required to contain the breach and mitigate effects.
  - A formal review and necessary procedural changes must be implemented to prevent recurrence

17. Publication of information

The Trust and its schools are committed to transparency and fulfilling their obligations under the Freedom of Information Act 2000 (FOIA).

The Trust has formally adopted the Information Commissioner's Office (ICO) Model Publication Scheme. This scheme specifies the seven classes of information that the Trust and its schools will proactively make available to the public.

Classes of information routinely published include key policies, governance structures, financial reports, and regulatory information. A guide to the information available under this Publication Scheme is accessible on the Trust and school websites.

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust or school's processes make it necessary.

19. Monitoring Arrangements

Advice will be sought from the DPO in reviewing this policy to ensure it meets latest legislation and guidance.

This policy will be reviewed annually and approved by the Audit, Risk and Compliance Committee.