LIGHTHOUSE SCHOOLS PARTNERSHIP

DATA PROTECTION POLICY

(INCORPORATING SPECIAL CATEGORIES)

Statutory

Policy Approved by the Board of Trustees	
Signed: **Name: Adele Haysom** **Chair of Board of Trustees**	**Date: 27 January 2026**
Authorised for Issue	
Signed: **Name: Gary Lewis** **Chief Executive**	**Date: 27 January 2026**

Document History

Version	Author/Owner	Drafted	Comments
1.0	Clare Sanders/TJM	June 2016 Published 3-August 2016	Based on Gordano School model – original source not recorded
2.0	Louise Malik/Tim Monelle	August 2018	Updated to reflect GDPR and latest requirements
3.0	Louise Malik/Tracey Joyce	August 2020	To reflect i-West template and general updates
4.0	Louise Malik/Neill Bird	August 2022	Privacy Notice and other updates, including new appendix

			5 and general best practice guidance
5.0	Louise Malik/Trust Services	Sept 2024	Minor changes to names, contacts and definitions
6.0	Louise Malik/Trust Services	January 2026	Addition of right to complain, in accordance with DUAA, as well as a reference to AI tools under Automated Decision Making. Addition of reference to recognised legitimate interests.

Review cycle	Biennial
Next Review date	January 2028

This policy applies to all schools and employees within the Lighthouse Schools Partnership.

This policy remains valid, and in operation, until a new or updated policy is published.

Contents

1. Aims 4
2. Scope 4
3. Distribution 4
4. Definitions 4
5. Roles and Responsibilities 6
6. Data Protection Officer (DPO) 7
7. Data Subject Rights 8
8. Data Protection Principles 10
9. Processing Personal Data 12
10. Third Parties with Access to Personal Data 14
11. Data Protection by Design and Default 15
12. Personal Data Breaches or Near Misses 16
13. Biometric Recognition Systems 16
14. Destruction of Records 16
15. Training 17
16. Monitoring Arrangements 17
17. Complaints 17
18. Legislation and Guidance 18
19. Links with Other Policies 18
Appendix 1 – Examples of Special Category Data that we Process 19
Appendix 2 – Subject Access Request Procedure (SAR) 20
Appendix 3 - Information Potential Data Breach Response Incident Form 21
Appendix 4 – Data Protection Complaint Form 23
Appendix 5 – GDPR Walkabout Checklist 26
Appendix 6- Privacy Notice for Pupils and Parents 28
Appendix 7 - Privacy Notice for Job Applicants 28
Appendix 8 - Privacy Notice for Students 28
Appendix 9 – Privacy Notice for School Workforce 28
Appendix 10 – Privacy Notice for Visitors 28
Appendix 11 – Consent for processing Personal Data for Early Years and Primary Aged Children 28
Appendix 12 – Consent for use of Workforce Images 28
Appendix 13 - Consent for Processing Personal Data for Pupils in Key Stage 3 and 4 28

1. Aims

Lighthouse Schools Partnership (the Trust) is committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Data (Use and Access) Act 2025 (DUAA), as applicable. The Trust is registered as a data controller with the Information Commissioner.

Details of the Trust's Data Protection Officer (DPO) can be found at section 6.

2. Scope

This policy applies to all Schools and employees within the Lighthouse Schools Partnership. This policy applies to anyone who has access to data and/or is a user of the Trust's Information and Communication Technology (ICT) systems, including staff, trustees, governors, students, volunteers, parents/carers, visitors, contractors, and other community users.

This policy is also intended to serve as the Appropriate Policy Document for the processing of special category data and criminal offence data (where applicable).

This policy applies to all personal data for which Lighthouse Schools Partnership is the data controller, regardless of whether it is in paper or electronic format.

3. Distribution

This policy is available on the Trust's website and in hard copy from the Trust or individual school offices.

4. Definitions

Personal Data - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. We may process a wide range of personal data of staff (including volunteers) as part of our operation. A non-exhaustive list of examples of the types of personal data that we process may be found in our Privacy Notices.

Special Category Data - Formerly known as "sensitive personal data", special category data is information that is a lot more sensitive to that person and needs more protection. These are:

- racial or ethnic origin
- political opinions

- religious/philosophical beliefs
- trade union membership
- genetic data
- biometric data (for identification purposes)
- health data (mental and physical)
- sex life or sexual orientation

Examples of the types of special category data we process can be found at Appendix 1. Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as do our Privacy Notices which can be found on Trust/School websites.

Data Subject(s) - The data subject is the person about whom the personal data relates or identifies.

Data Processing - Data processing is an over-arching term that means "doing something" with personal data. This commonly includes:

- Collecting or collating the data
- Analysing the data
- Sharing the data
- Storing the data
- Destroying the data

Data Controller - The data controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that the organisation undertakes. They will make all the decisions about what is captured, how it's used and the purpose for it, as well as deciding what controls need to be in place.

Data Processor – The data processor is occasionally a person, but more commonly an organisation commissioned by a data controller to carry out their data processing on behalf of the data controller. These are often software providers such as Microsoft or contracted out services such as an insurance company. Essentially, a data processor is acting as an extension of the data controller, so must operate under the data controller's instructions and under the terms of a data processing agreement (contract).

Data Sharing – Data sharing means *giving* data to another data controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the data controller of that information and therefore makes the decisions over what they will do with it.

Note, we do NOT *share* data with our data processors, as they are processing it under our data controllership.

Data Breach - The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example sending an email to the wrong recipient, losing a file containing personal data, or sharing passwords enabling someone else to access your account. However, we consider any failing of one of

the data protection principles (Article 5 of UK GDPR) as a breach of data protection legislation, so could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of UK GDPR).

Data Processing Agreement – This is a legally binding contract between the data controller and its data processor. This contract defines exactly how the data controller expects the data processor to process its personal data and follow standard contract clauses.

Data Sharing Agreement – This is a non-legally binding written agreement between data controllers where there is regular sharing of personal data. The data sharing agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, how the data will be shared.

Data Protection Officer – See section 6 for details.

5. Roles and Responsibilities

Governing Bodies - The Board of Trustees and Local Governing Bodies (LGB) have overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

Data Protection Lead - Headteachers act with the delegated authority of the LGB on a day-to-day basis and will liaise with the Data Protection Officer (DPO). In the Headteacher's absence, in case of emergency, this role will be delegated to School Business Managers/Office Managers.

All other staff (as defined in scope) - All staff are responsible for:

- Familiarising themselves with and complying with this policy and any related policies. The learning culture within the organisation seeks the avoidance of blame and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Completing required GDPR training (see section 15 for details);
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by the Trust/School for accessing and processing personal data ensuring that they are properly "logged-off" at the end of any session in which they are using personal data, and locking devices when they are temporarily left unattended at any point (Windows Button + L is a handy shortcut);

- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite (unless in accordance with the guidelines at section 8) or to personal devices other than in accordance with the School's E-Safety/On-Line Safety Policies which include Bring Your Own Device guidance.
- Deleting any data they hold in line with the Records Management Policy;
- Informing the Trust/School of any changes to their personal data, such as a change of address;
- Reporting to the Line Manager, Headteacher, Deputy or Business/Office Manager, or in their absence the DPO (using the dpo@lsp.org.uk email address, copying in the Headteacher for school-based staff), in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to section 12 of this policy;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required and potentially a Data Protection Impact Assessment (DPIA), please see – *Third Parties with Access to Personal Data* (section 10 of this policy).

6. Data Protection Officer (DPO)

The DPO is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance to the Board of Trustees and, where relevant, provide the Trust/School with advice and recommendations on data protection issues.

Lighthouse Schools Partnership has appointed One West as its DPO, and they can be contacted by email at:

One West (Bath and North-East Somerset Council)	Email: i-west@bathnes.gov.uk Telephone: 01225 395959

Guildhall, High Street, Bath, BA1 5AW

Under usual circumstances, the Headteacher, a member of the Senior Leadership Team (SLT) or Trust Services will be the point of contact with the DPO.

7. Data Subject Rights

In all aspects of its work, the Trust/School will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the Trust's work. Subject to exceptions, the rights of the data subject as defined in law are:

7.1 Right to be informed

The Trust advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

7.2 Right of access

An individual when making a Subject Access Request (SAR) is entitled to the following;

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

The Trust/School must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by up to a further two calendar months.

7.3 Right to Rectification

Individuals have the right to ask us to correct information they think is inaccurate or incomplete. The Trust/School has a duty to investigate any such claims and rectify the information where appropriate within one calendar month, unless an extension of up to a further two calendar months can be justified.

7.4 Right to erasure

Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

- The information was given voluntarily; consent is now withdrawn and no other legal basis for retaining the information applies;
- The information is no longer required;
- The data was collected from a child for an online service; or
- The Trust/School has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it

concludes that the rights of the individual to have the data erased outweigh those of the Trust/School to continue to process it.

The Trust/School will consider such requests as soon as possible and within one month, unless it is necessary to extend that timeframe for a further two months on the basis of the complexity of the request or because a number of requests have been received from the individual.

7.5 Right to restrict processing

This is not an absolute right. An individual may ask the Trust/School to temporarily limit the use of their data (for example, storing it but not using it) when it is considering:

- A challenge made to the accuracy of their data, or
- An objection to the use of their data.

An individual may also ask us to restrict the destruction of a record, if they wish it to be retained beyond the normal retention period.

In addition, the Trust/School may be asked to limit the use of data rather than delete it:

- If the individual does not want the Trust/School to delete the data but does not wish it to continue to use it;
- In the event that the data was processed without a lawful basis;
- To create, exercise or defend legal claims.

7.6 Right to data portability

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The Trust/School only has to provide the information where it is electronically feasible.

7.7 Right to object

Individuals have a right to object in relation to the processing of data in respect of:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes;
- a task carried out for the exercise of official authority;
- a task carried out in its legitimate interests;
- scientific or historical research, or statistical purposes, or
- direct marketing.

Only the right to object to direct marketing is absolute, other objections will be assessed in accordance with data protection principles. The Trust/School will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress.

7.8 Right to complain

Individuals have the right to complain about the way in which an organisation processes their personal data. This is the first stage, before the Information Commissioner will consider a personal data complaint. See section 17 for further details.

7.9. Rights related to automated decision making

This does not apply as the Trust/School do not currently employ automated decision-making processes.

8. Data Protection Principles

Data protection legislation is based on seven key data protection principles that the Trust/School complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the Trust/School will explain to individuals why it needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). The Trust/School reviews its documentation and the basis for processing data on a regular basis.
- **Collected for specified, explicit and legitimate purposes** – the Trust/School will explain these reasons to the individuals concerned when it first collects their data (for example via Data Collection Sheets or Consent Forms). If the Trust/School wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. In which case, the Trust/School will document the basis for processing.
- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed** – the Trust/School must only process the minimum amount of personal data that is necessary in order to undertake its work.
- **Accurate and, where necessary, kept up to date** – the Trust/School will check the details of individuals on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- **Kept for no longer than is necessary for the purposes for which it is processed** – the Trust/School will review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (RoPA) (or sooner if needed). When the Trust/School no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the Records Management Policy. We will only keep personal data, including special category data, in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;

- The Records Management Policy governs how long all data, including special category data, shall be retained for. This policy is complied with and reviewed regularly;
- Once the data is no longer needed, we will delete it, securely destroy it in line with our Records Management Policy, or render it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – the Trust/School will implement appropriate technical measures to ensure the security of data and systems for staff and all users;
  - We will adopt a risk-based approach to taking data offsite. Unless absolutely necessary, hard copies of special category data will not be removed from our premises.
  - Any decision to remove the information will be based on the business needs of the organisation or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any special category data to be accessed via appropriately encrypted means rather than hard copy, when off-site.
  - If there is no reasonable alternative to removing hard copies from the Trust/School site, the following procedure will apply:
    i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data in school trip packs;
    ii. Information will be transported and stored in a lockable case;
    iii. Wherever possible, information that is removed from site will be pseudonymised by using a "key" held by the office on site;
    iv. We will adopt a risk-based approach, for example hard copy personal data with lower sensitivity (e.g. exercise books) may be taken off site, but if left in a vehicle will be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special category data (e.g. SEND, safeguarding, health data) will be kept on the staff member's person at all times;
    v. Special category data will be returned to the Trust/School premises at the end of the working day, if not on a residential school trip. If this is not practicable, and a staff member needs to retain the information in their personal possession, this will be discussed in advance with a member of SLT including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the SLT will record their decision;
    vi. Data will be tidied away when not in use (e.g. when staff undertake working at home, it will be out of sight of family members and tidied away afterwards);

vii. Only those who need to access the data concerned will be granted permission and access to it;

- **Accountability** - The Trust/School will comply with its obligations under data protection laws including the UK GDPR and be able to demonstrate this via the measures set out in this policy including completing Data Protection Impact Assessments (DPIAs) where necessary; integrating data protection into internal documents, including this policy, any related policies and Privacy Notices; regularly training members of staff on all relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance using the annual compliance report and/or risk register.

9. Processing Personal Data

In order to ensure that the Trust/School processing of personal data is lawful, it will always identify one of the following six grounds for processing **before** starting the processing:

- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent. We will seek consent (where appropriate) to process data from the individual or parent, depending on their mental capacity to understand what is being asked for;
- The data needs to be processed so that the Trust/School can fulfil a **contract** with the individual, or the individual has asked the Trust/School to take specific steps before entering into a contract;
- The data needs to be processed so that the Trust/School can comply with a **legal obligation**;
- The data needs to be processed to ensure the **vital interests** of the individual, i.e. to protect someone's life;
- The data needs to be processed so that the Trust/School, as a public authority, can **perform a task in the public interest, or carry out** its **official functions**;
- The data needs to be processed for the **legitimate interests** of the Trust/School or a third party where necessary, balancing the rights of the individual (unless the processing is necessary for a 'recognised' legitimate interest). However, where the Trust/School can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

9.1 Processing Special Category Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the UK GDPR. The grounds that we may rely on include:

a) The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment and social security and social protection law and research***; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018;
c) Processing is necessary to protect the **vital interests** of the individual or of another where the individual is physically or legally incapable of giving consent;
d) Processing is carried out in the course of its legitimate activities by a **not-for-profit organisation** with a political, philosophical, religious, or trade union aim on the condition that the processing relates solely to its members, or former member who have regular contact with it, and that the personal data is not disclosed outside that body without consent.
e) Processing relates to personal data which is **manifestly made public** by the individual;
f) Processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity;
g) Processing is necessary for reasons of **substantial public interest*** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision- making process.

   These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

   - Statutory and government purposes
   - Safeguarding of children or individuals at risk
   - Legal claims
   - Equality of opportunity or treatment
   - Counselling
   - Occupational pensions

h) Processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of **health or social care** or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i) Processing is necessary for reasons of **public interest in the area of public health***;

j) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the DPO where appropriate.

* We will also comply with Schedule 1 of the Data Protection Act 2018 (as well as Article 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest.

9.2 Legal basis for processing criminal offence data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

We will not maintain a register of criminal convictions.

When processing this type of data, we will most likely rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection;
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual;
- The processing is necessary for statutory purposes; or
- Consent – where freely given. The Trust/School acknowledges because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other grounds apply.

10. Third Parties with Access to Personal Data

Please refer to our Privacy Notices for details of who, aside from Lighthouse Schools Partnership, has access to the personal data processed.

10.1 Data Sharing

Lighthouse Schools Partnership will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

- The Trust/School will share data if there is an issue with an individual or third party, for example a parent/carer that puts the safety of staff or others at risk;
- The Trust/School will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the

"Seven golden rules of information sharing." In limited circumstances, data may be shared with external agencies without the knowledge or consent of the parent or child in line with the Data Protection Act 2018, which includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent;

The Trust/School may also disclose personal data to law enforcement and government bodies where there is a lawful requirement/basis for us to do so, including:

- For the prevention or detection of crime and/or fraud;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided, or it is otherwise fair and lawful to do so.

The Trust/School may also share personal data with emergency services and local authorities to help them to respond to an emergency situation.

10.2 Third-Party Processors

Lighthouse Schools Partnership's suppliers and contractors, including its DPO and IT provider, may need access to data to provide services. When third parties are processing personal data on behalf of us, we will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data disclosed;
- Only provide access to data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working.

11. Data Protection by Design and Default

The Trust/School has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by a Data Protection Impact Assessment (DPIA). Prior to the commencement of any such activity, the DPO will be consulted and an initial screening will be conducted to assess risk.

12. Personal Data Breaches or Near Misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident or a "near-miss" has occurred, the staff member will inform the Headteacher. A data breach form will be completed and sent to the DPO (i-west@bathnes.gov.uk) **immediately,** copying in dpo@lsp.org.uk. The DPO will assess whether the ICO should be informed (within 72 hours as is legally required), and/or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

A log will be kept recording all breaches and near misses.

13. Biometric Recognition Systems

Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form of fingerprint, voice, or facial recognition. We will use biometric data to enable payment of school meals.

We will undertake a Data Protection Impact Assessment (DPIA) before implementing any new biometric system, to assess the impact on individuals.

In the case of adults, for example staff members, we will seek their consent before processing any biometric data.

In accordance with the Protection of Freedoms Act 2012, in the case of children, we will notify all those with parental responsibility in the case of any individual under 18, unless this is impractical (for example the whereabouts of the parent is unknown or if there is a safeguarding issue) and may only proceed if we have at least one positive written consent, and no written parental objection. We will not proceed to process the information if the child themselves objects. Either parents or the child may withdraw their consent at any time.

If the individual concerned does not agree to proceed or wishes to withdraw their consent to the use of the biometric system, we will provide an alternative means of achieving the same aim.

14. Destruction of Records

The Trust/School adheres to its Records Management Policy and will permanently destroy both paper and electronic records securely in accordance with these timeframes.

We will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

Where we delete electronic records and our intention is to put them beyond use, even though it may be technically possible to retrieve them, we will follow the Information Commissioner's guidance on deleting data and this information **will not** be made available on receipt of a Subject Access Request (SAR).

15. Training

To meet its obligations under data protection legislation, the Trust/School will ensure that all staff, volunteers, and governors receive an appropriate level of data protection training as part of their induction. Permanent members of staff will receive computer based data protection training at least every 3 years and informal refresher training throughout the year. Those who have a need for additional training will be provided with it, for example relating to use of systems or their role responsibilities, such as being an internal data protection lead.

Data protection also forms part of continuing professional development. Staff members will undertake regular informal discussions on data protection, to ensure key updates are provided where changes to legislation, guidance or the Trust's/school's processes make it necessary. This will include lessons learned from data breaches and near misses, preventative measures to avoid them, and other best practice as advised.

16. Monitoring Arrangements

Whilst the DPO will be responsible for advising on the implementation of this policy and monitoring the Trust/School overall compliance with data protection law, the Trust/School will be responsible for the day-to-day implementation of the policy and for making the DPO aware of relevant issues which may affect the Trust's/school's ability to comply with this policy and the legislation.

This policy will be reviewed every two years, unless an incident or change to regulations dictates an earlier review.

17. Complaints

The Trust/School will always seek to implement best practice and strive for the highest standards. The Trust will operate an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The Trust/School complaints policy can be found on its website.

Individuals have the right to make a complaint to us about the way in which we process personal data. There is also a right to make a complaint to the Information Commissioner, but complaints should be raised with us first by contacting us at dpo@lsp.org.uk . We will acknowledge any complaint within 30 days and respond without undue delay.

We have provided an electronic form for individuals to make a complaint, which can be found here. A pdf form can also be found at Appendix 4.

The ICO is contactable at:

www.ico.org.uk

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

18. Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Data (Use and Access) Act 2025 (DUAA)
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office

19. Links with Other Policies

This Data Protection Policy is linked to the following:

- Records Management Policy
- Safeguarding Policy
- Acceptable Usage Policies
- E-Safety/Online Safety Policies to include Bring Your Own Device guidance
- Privacy Notices

Appendix 1 – Examples of Special Category Data that we Process

Examples of where we may process special category data include:

Employee health data and information concerning their racial/ethnic origin

Pupil health data and information concerning their racial/ethnic origin in admissions records and in pupil records/school trip packs

Special Educational Needs information

School census information

Attendance records

Biometric data e.g. fingerprints for cashless catering/door entry systems

Information contained within child protection and safeguarding records

Staff, Governor, Trustee and Volunteer application forms

HR files including disciplinary and capability proceedings which may include DBS, and right to work checks, health, and equal opportunities data (disability, race, ethnicity, sexual orientation).

Accident reporting documentation

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice(s) which can be found on our website.

Appendix 2 – Subject Access Request Procedure (SAR)

Lighthouse Schools Partnership will complete the following steps when processing a request for personal data (Subject Access Request, or SAR) with advice from its DPO.

1. Ascertain whether the requester has a right to access the information and capacity.
2. Obtain (reasonable and proportionate) proof of identity.
3. Engage with the requester if the request needs clarifying.

   Nb only once steps 2 and 3 have been completed, can the "clock" start.
4. Make a judgement on whether the request is complex and therefore can be extended by an additional two months.
5. Acknowledge the requester providing them with:
   a. the response time – one calendar month (as standard), an additional two months if complex; and
   b. details of any costs – free for standard requests, or we can charge, or refuse to process, if the request is manifestly unfounded or excessive, or if further copies of duplicate information is required. The fee must be in line with the administrative cost.
6. Use its Record of Processing Activities (RoPA) and/or data map to identify data sources and where they are held.
7. Collect the data (the organisation may use its IT support to pull together electronic data sources such as emails and databases).
8. If (6) identifies third parties who process it, then engage with them to release the data to Lighthouse Schools Partnership.
9. Review the identified data for exemptions and redactions in line with the ICO's Guide to the Right of Access and in consultation with the organisation's DPO (One West).
10. Create the final bundle and check to ensure all redactions have been applied.
11. Submit the final bundle to the requester in a secure manner and in the format they have requested.

Appendix 3 - Information Potential Data Breach Response Incident Form

This document provides the documented evidence and audit trail of a reported potential data breach. It is designed to operate alongside the Data Protection Policy, and personal data breach reporting process.

This form is to be completed by the Incident Handler(s) in the school. The Incident Handler will usually be the Headteacher.

The incident may require additional input and support from other organisations such as Information and Communication Technology (ICT), the school's Data Protection Lead, the DPO and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation *If there was any delay in reporting the incident, please explain why this was*	
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why? *Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes*	
2. Recovery of the data	
What have you done to contain the incident? *eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*	
Please provide details of how you have recovered or attempted to recover the data, and when *Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*	
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals (include consideration of mental health or other vulnerabilities of individuals impacted by the data breach.)? What steps have been taken / planned to mitigate the effect?	
Your name and contact details:	

Please email any breach or potential breach within 72 hours of its discovery (whenever possible) to i-west@bathnes.gov.uk and cc dpo@lsp.org.uk

LIGHTHOUSE SCHOOLS PARTNERSHIP

Appendix 4 – Data Protection Complaint Form

Make a complaint about how we use your data
Under data protection legislation, organisations that collect and use personal information have to follow rules of good practice for handling such data. The law also gives rights to individuals whose information they keep. These rights include the right to complain should you believe your personal data has been processed inappropriately.

What you can complain about
You can complain to us if you have been denied any of your rights under data protection legislation. This includes your right to see the information an organisation holds about you, or if the information about you is used, held or disclosed either unfairly, for a reason that is not the one it was collected for, or without proper security. Or, if the information about you is inadequate, irrelevant or excessive, inaccurate or out of date, or kept for longer than is necessary. You can also complain if you feel we have not provided you with all relevant information as part of a Subject Access Request (SAR).

How to make a complaint about data protection
If you want to make a complaint about our service, then you should do so **within three months**. Waiting longer than that will affect our ability to look into your complaint and is likely to mean that we will not be able to consider the matter at all. Make it clear that the matter concerns data protection and provide as much detail as you can. Tell us your name and how to contact you. You can also attach any documents relevant to your complaint.

Make a complaint
To make a complaint, please complete the form below.

What happens next
Your complaint will be treated confidentially, and we will acknowledge receipt within 30 days. We will do a full investigation and will respond to you without undue delay, providing updates to you as we progress. We may need to contact you if the complaint needs to be clarified, to ensure that we are able to fully consider the complaint.

If you are not happy with our response
If you are not satisfied with our response, you may wish to refer it to the Information Commissioner at www.ico.org.uk/make-a-complaint

Data Protection Complaint Form

This form can be completed by hand and a copy emailed to dpo@lsp.org.uk, or can be posted to Trust Services, Lighthouse Schools Partnership, Gordano School, St Mary's Road, Portishead, BS20 7QR.	
Name of school/organisation about whom you are complaining	
Your name	
Your contact details (how you would like us to respond to you)	
Full name of pupil (if relevant to your complaint)	
Name of contact (if you have already discussed the matter with a member of staff at the school or Lighthouse Schools Partnership)	
Details of your complaint (explaining clearly and simply what has happened)	*(Continue overleaf if needed…)*
Details of additional documents provided (if any)	

Declaration

You must read the Privacy Notice and sign to agree to the declarations below to use this form.
(The Privacy Notice can be found at www.lsp.org.uk/page/?title=Policies&pid=23)

- I have read the Privacy Notice
- The information I have provided is accurate, to the best of my knowledge
- I understand that Lighthouse Schools Partnership will store the information relating to my complaint electronically and/or in hardcopy, including any documents I have provided, and keep these records for three years following closure of the complaint

Signed …….

LIGHTHOUSE SCHOOLS PARTNERSHIP

Appendix 5 – GDPR Walkabout Checklist

Good data protection practices should be ingrained into the ethos of the Trust/School. This check sheet must be completed at least annually, to ensure best practice guidance is being followed, and any potential risks are highlighted. It may be done at the same time as one of the termly Health & Safety Inspections.

Name of Trust/School being reviewed	

Issues to look out for	**Observations**	**Follow-up actions**
School-wide		
Paperwork, including small notes, left out on desks		
Unattended computer screens left unlocked		
Photos of pupils, together with full names and / or school year on display		
Full or over-flowing paper / confidential waste bins		
Screens facing windows		
Prints left at printers / photocopiers		
Reception / Office		
Excessive or personal information on display within the visitor book		
Pupil late sign-in book completed by pupils or parents		
Contact lists with personal phone numbers next to phones		

Sensitive or confidential information left in pigeonholes		
Sensitive phone calls being made in earshot		
Photos/names of people who aren't allowed to pick up pupils on display in the reception areas		
Confidential waste awaiting collection / shredding unsecured		
Medical alert information unsecured		
Classrooms		
Birthday 'trees' with excessive information (ie full names and birthdate)		
Class lists left unsecured		
Miscellaneous		
Any personal information on display in areas that are privately hired out		
Allergy information left out in the kitchen or other areas		
First aid book / forms left unsecured		
SENCO office and / or contents left unsecured		
Network server cabinet left unlocked (or key left in lock)		
Archive stores unsecured		

Name of person/s completing this form		**Date**	

If you have any specific queries or concerns relating to data protection, please contact the school's Data Protection Lead or otherwise the Trust Data Protection Officer i-west@bathnes.gov.uk

Data Protection Policy

Appendix 6- Privacy Notice for Pupils and Parents

This appendix is a separate file.

Appendix 7 - Privacy Notice for Job Applicants

This appendix is a separate file.

Appendix 8 - Privacy Notice for Students

This appendix is a separate file.

Appendix 9 – Privacy Notice for School Workforce

This appendix is a separate file.

Appendix 10 – Privacy Notice for Visitors

This appendix is a separate file.

Appendix 11 – Consent for processing Personal Data for Early Years and Primary Aged Children

This appendix is a separate file.

Appendix 12 – Consent for use of Workforce Images

This appendix is a separate file.

Appendix 13 - Consent for Processing Personal Data for Pupils in Key Stage 3 and 4

This appendix is a separate file.