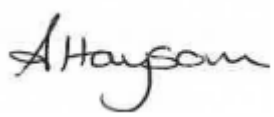
LIGHTHOUSE SCHOOLS PARTNERSHIP

DATA PROTECTION POLICY

Statutory

Policy Approved by the Board of Trustees

Signed: 

Date: 03/11/22

Name: Adele Haysom

Chair of Board of Trustees
Authorised for Issue

Signed: 

Date: 03/11/22

Name: Gary Lewis

Chief Executive

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

Date Policy Adopted	03/11/22
Review cycle	Biennial
Review date	Autumn Term 2024

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

DATA PROTECTION POLICY (INCORPORATING SPECIAL CATEGORIES)

Contents

1. Aims

The Lighthouse Schools Partnership 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 (UKGDPR) and the Data Protection Act 2018 (DPA 2018).The Trust is registered as a data controller with the Information Commissioner.

The details of the Trust's Data Protection Officer can be found at paragraph 6.

2. Scope

This policy applies to anyone who has access to and/or is a user of Trust's ICT systems, both in and out of the Trust, including staff, governors, students, volunteers, parents / carers, visitors, contractors, and other community users.

This policy applies to all personal data, 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

Term	Definition
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. The School may process a wide range of personal data of staff (including governors and volunteers) students, their parents or guardians as part of its operation. This personal data may include (but is not limited to): • Names and addresses (including email addresses) • Bank details • Academic data e.g. class lists, pupil / student progress records, reports, disciplinary actions, admissions and attendance records • References • Employment history • Taxation and national insurance records

	• Appraisal records • Identification number • Location data
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
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 of 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.

5. Roles and Responsibilities

Trustees/Local Governing Bodies (LGB) - The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations. LGBs have responsibility for ensuring that their school(s) complies with the policies and procedures established by the Trust.

Head of Trust Services - The Head of Trust Services acts as the representative of the data controller on a day-to-day basis.

Headteachers - The Headteacher acts with the delegated authority of the Local Governing Body on a day to day basis and will liaise with the DPO, in conjunction with the Head of Trust Services. In the Headteacher's absence, in case of emergency, this role will be delegated to the Deputy Headteacher or the School Business Manager. Headteachers are responsible for ensuring that the Trust's data protection policies and procedures are implemented and maintained in their school(s) and that staff and LGB members have sufficient knowledge and training to carry out their responsibilities.

All staff - This policy applies to all staff employed by the Trust, and to external organisations or individuals working on behalf of the Trust. Staff who do not comply with this policy may face disciplinary action.

All staff are responsible for:

- Familiarising themselves with and complying with this policy and acceptable use policies for staff. 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. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- 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 school/Trust 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;
- 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 Bring Your Own Device policy
- Deleting data in line with this policy and the Records Management Policy;
- Informing the School of any changes to their personal data, such as a change of address;
- Reporting to the Line Manager, Headteacher, Deputy or Business 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 the section 13 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 likely to be required and potentially a data protection impact assessment, please see - Sharing Personal Data (section 10 of this policy).
- in cases where they are given, or asked to process or store, any information that is not covered by the authority of the DPO or the trust under this policy

- Providing access to emails to support a SAR as required. IT support will be used to gain access where it is not granted.

6. Data Protection Officer (DPO)

The Data Protection Officer (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 directly to the Board of Trustees and, where relevant, provide the Trust with advice and recommendations on data protection issues.

The Trust has appointed i-west to act as the DPO for a 3 year period from 1st June 2020. Full details of the DPO's service are set out in a Service Level Agreement (SLA) which is available on request.

i-west contact details are provided below:

Email: DPO@LSP.org.uk

Telephone: 01225 395959

One West (iWest)
Bath and North East Somerset Council
Guildhall
High Street
Bath
BA1 5AW

Under usual circumstances the internal data protection lead, Headteacher or a member of SLT will be the point of contact with the DPO.

It is recommended to for the internal Data Protection Lead to create an account to enable them to log into the iWest website and also familiarise themselves with the content, including the GDPR documentation and advise available.

7. Subject Access Requests and Other Rights of Individuals

In all aspects of its work, the Trust 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:

a) The 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.

b) The Right of access

An individual when making a subject access request (SAR) is entitled to the following;

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

The School must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by a further 2 calendar months. Please refer to Appendix 2 for further details as to how to manage a subject access request.

c) The Right to rectification

Individuals have the right to ask us to rectify information that they think is inaccurate or incomplete. The 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 2 calendar months can be justified.

d) The 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 by the School;
- A legal obligation to erase the data applies;
- The data was collected from a child for an online service or
- The 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 School to continue to process it.

The 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 a number of requests have been received from the individual.

e) The Right to restrict processing

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

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

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

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

f) The 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 School only has to provide the information where it is electronically feasible.

g) The 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 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 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.

h) Rights related to automated decision making

Individuals have a right to request information on whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access

request, or have given their consent; or it must be evident that it is in the best interests of the child, taking into account things such as the nature of the personal data and any duty of confidence owed, any court orders that may apply, and any consequences of allowing those with parental responsibility access to the information or detriment to the child of not permitting access.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at a Trust Primary school may be granted without the express permission of the pupil subject to the evaluation described above. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils above this age in a Trust Secondary school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

8. Data Protection Principles

The UKGDPR is based on 7 key data protection principles that the Trust complies with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner – the School/Trust 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 School/Trust reviews its documentation and the basis for processing data on a regular basis.

- Collected for specified, explicit and legitimate purposes – the School/Trust explains these reasons to the individuals concerned when it first collects their data (for example via Data Collection Sheets or Consent Forms). If the School/Trust 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. The School/Trust will document the basis for processing.

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed - the School/Trust 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 School/Trust will check the details of those 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 – We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When the School/Trust 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 only keep personal data, include 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;

    - We have a Records Management Policy which 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 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 School implements appropriate technical measures to ensure the security of data and systems for staff and all users. Where special category data is stored electronically, for example in SIMS or CPOMS, permissions will be assigned to staff logins to ensure that the data is not accessible to all staff, but only to those with specific authorisation and purpose. Please refer to the schools other policies such as E-Safety, staff acceptable use policy and bringing your own device policy, and how data is securely transferred in and out of the school's system.

  We adopt a risk- based approach to taking data offsite. Unless absolutely necessary, hard copies of special category personal data will not be removed from our premises.

  Any decision to remove the information must be based on the business need 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 personal data to be accessed via an appropriately encrypted means rather than via hard copy, when off-site.

  If there is no reasonable alternative to removing hard copies from the School/Trust 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 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 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 must 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) must be kept on the staff member's person at all times.

v. Special category data must be returned to the School's 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 must 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 must record their decision.
vi. Data will be tidied away when not in use (e.g. when staff undertake marking at home, it must be out of sight of family members, not left out and tidied away afterwards).
vii. Only those who have need to access the data concerned will be granted permission and access to it.
viii. Policies such as our acceptable use and bring your own device policies describe the requirements around, remote working and password protection

- Accountability - The School complies with its obligations under data protection laws including the UKGDPR and can demonstrate this via the measures set out in this policy including:

  - Completing Data Protection Impact Assessments (DPIAs) where the School/Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. This largely involves special category personal data and CCTV. However, the School will liaise with the DPO who will advise on this process. A template is available from iWest's members area of their website. Any activity involving the processing of personal data must be registered on the Register of Processing Activity and reviewed, at the very least, annually;
  - 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. It is recommended that schools deliver in-house GDPR training annually. iWest have training available to support this process which, together with other training resources and awareness is available on Foldr. The school also maintains a record of attendance. Staff who process special category data, will be provided with such additional training as appropriate for example on safeguarding systems. Records of training are maintained;
  - Regularly conducting reviews and audits to test its privacy measures and ensure compliance with relevant legislation and school policies. As part of this a documented walk of all school buildings is to be taken at least annually, with the findings recorded on the GDPR walkabout checklist (see appendix 5) and submitted on Every;
  - Maintaining records of its processing activities for all personal data that it holds;
  - Policies related to the handling of data and associated documentation will be regularly reviewed on a rolling basis and updated in accordance with new

guidance, legislation and practice. They will be publicised to staff who will be required to familiarise themselves with them;
- The Record of Processing Activities (a template is available from iWest's members area of website) will be maintained and reviewed at least annually;
- Where any breaches of personal data have occurred, the reasons for this will be reviewed and changes made to practice and procedure as appropriate;
- Stakeholders will manage risks and compliance using the annual compliance statement provided by the Data Protection Officer and/or a Risk Register.

9. Processing Personal Data

In order to ensure that the Trust's processing of personal data is lawful; it will always identify one of the following six grounds for processing before starting the processing:

- The data needs to be processed so that the Trust 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 Trust can comply with a legal obligation;
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life;
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions;
- The data needs to be processed for the legitimate interests of the Trust or a third party where necessary, balancing the rights of freedoms of the individual). However, where the Trust can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.
- The individual (or their parent/carer when appropriate in the case of a pupil/ student) has freely given clear consent. In the case of special categories of personal data, this must be explicit consent. The Trust will seek consent to process data from the pupil / student or parent depending on their age and capacity to understand what is being asked for.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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 UKGDPR. 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, health 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.

Health or social care purposes includes the following purposes:

i. Preventative or occupational medicine
ii. The assessment of the working capacity of the employee

c) Processing is necessary to protect the vital interests of the individual or of another individual where the individual is physically or legally incapable of giving consent;

d) Processing relates to personal data which are manifestly made public by the individual;

e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

f) 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

g) 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;

h) Processing is necessary for reasons of **public interest in the area of public health;**

i) 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 Data Protection Officer where appropriate.

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

Legal basis for processing criminal offence data

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

We do not maintain a register of criminal convictions.

When processing this type of data, we are most likely to 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; or
- Consent – where freely given. The Trust 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 ground applies.

10. Sharing Personal Data

Please refer to the School/Trust's Privacy Notice(s).

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

- The Trust will share data if there is an issue with a student /pupil or third party, for example a parent/carer, that puts the safety of staff or others at risk;
- The Trust will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate, outlining the reasons and protections around this data sharing, before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing" which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or student;
- The Trust's suppliers and contractors including its data protection officer and IT providers may need data to provide services. When sharing data, the Trust will:
    - Only appoint suppliers or contractors which 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 it shares where there is regular sharing;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust;
    - Produce a Data Protection Impact Assessment where the type of data being processed could result in a high risk to the rights and freedoms of individuals.

Schools appointing suppliers and contractors and when setting up contracts will need to ensure that they comply with the above. The documents 'GDPR Contractor Agreement' and 'Third Party Questionnaire' will assist with this and can be found in Foldr.

The Trust may also share personal data with 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.

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils/students or staff.

Where personal data is transferred to a country or territory outside the UK or European Economic Area, the Trust will do so in accordance with data protection law. Further advice on this should be sought from the DPO.

11. Data Protection by Design and Default

The Trust 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 the Data Protection Impact Assessment. Prior to the assumption of any such activity the DPO must be consulted and an initial screening be conducted assessing risk.

12. 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.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key in buildings which are able to withstand at least a casual attack (e.g. not a timber shed or similar outbuilding) when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where any special category personal information needs to be taken off site, staff must sign it in and out from the Trust/school office (details of special category data can be found in the Privacy Notice for Pupils and Parents).
- Passwords that are at least eight characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Users are reminded to change their passwords at regular intervals and in accordance with any latest controlled version of the school's policy.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Only authorised removable media may be used and staff may not use their own personal removable media (such as USBs) unless they are encrypted and authorised by the school/Trust.

- Staff, pupils, Trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment and to adhere to the latest controlled version of the school's relevant technology polices e.g. acceptable use and bring your own device policy. This is detailed in the Acceptable Use Agreement that all staff are required to sign. This is also covered in the Code of Conduct Policy.
- Where we need to share personal data with a third party, we carry out a risk based assessment for each type of recipient, follow due process and take reasonable steps to ensure it is stored securely and adequately protected.

13. 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.

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will follow the procedure set out in Appendix 3 and 4.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Headteacher and DPO **immediately** in order that an assessment can be made as to 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.

To minimise data breaches and near misses it is strongly recommended that the following list of best practice actions is adopted by everyone:

DO

- If you are away from your screen lock it (**top tip;** use Windows Key + L as a shortcut).
- Put away sensitive files (e.g. SEN/Safeguarding/Payroll information) when you aren't using them.
- Only use first names (and surname initial if needed) where names are on display.
- On Birthday Charts don't show the exact dates – just the month is preferable.
- Dispose of personal data using a secure method like shredding or in confidential waste.
- Use 'strong' passwords

- Be aware of malicious emails, and be cautious with any unexpected links/attachments.
- Use Blind Copy (BCC) when emailing multiple external email addresses (e.g. parents).
- Setup an email sending delay to give you a safety net to react quickly to any errors.
- If in doubt with an email contact the sender by another trusted means e.g phone or SMS.

Additionally, if you are going off site make sure you:

- Take only the personal data you need.
- Where possible look to access/process data electronically – its more secure.
- Keep a log of any physical paper records that are taken offsite and check them back in when returned.
- When writing take measures where possible to de-personalise records – use initials not names.

DON'T

- Leave sensitive documents out on show wherever you are
- Reuse passwords across multiple sites/systems.
- Treat post as secure – if you must post sensitive data use recorded/special delivery.
- Click on links or open attachments on emails you were not expecting, or do not look and feel right.
- Use your laptop or PC in an area where the screen can be seen by unauthorised personnel.

If you are going off site, make sure you don't:

- Take more personal data than you need with you.
- Take sensitive and/or include special category data offsite unless essential and you have permission.
- Download or save electronic files to your personal device – use the schools network instead.
- Leave school email logged in on your personal device – its more secure to log in each time.

14. CCTV

The Trust may use CCTV in various locations across the Trust to ensure the safety and security of the sites and of all users of the sites. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the DPO using the DPO email address (DPO@LSP.org.uk).

The school will have a Data Protection Impact Assessment (DPIA) for any CCTV use

15. Photograph, Sound and Video Recording Consent

As part of our Trust/school activities, we may take photographs and record images of, or sounds from, individuals within our schools. This includes staff, volunteers, visitors, contractors, as well as pupils.

We will obtain written consent from parents/carers, or individuals aged 18 and over, for photographs, sound and videos to be taken for communication, marketing and promotional materials. Where we need parental consent (for pupils aged under 18), we will clearly explain how the photograph, sound and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent (for pupils aged 18 or over), we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within Trust/school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of the Trust/school by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust or school 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. Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and to have their personal data erased.

When using photographs, sound and videos in this way the Trust/school will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

Please see appendix 11 to 13 for our template consent forms.

16. 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 use biometric in the following ways:

pupils use fingerprints to receive school lunch instead of paying with cash

We will undertake a data protection impact assessment before implementing any new biometric system to assess the impact on individuals.

In accordance with the Protection of Freedoms Act 2012, once satisfied, we will notify all those with parental responsibility in the case of any student 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 student themselves objects. Either parents or the student may withdraw their consent at any time, although parents must object in writing.

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

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.

17. Destruction of records

The Trust adheres to its Records Management Policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes. 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, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files and biometric information. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. Where the School deletes electronic records and its intention is to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

18. Training

To meet its obligations under Data Protection legislation, the School/Trust will ensure that all staff, Trustees, Governors and Volunteers are provided with computer based data protection training as part of their induction process, with refresher training every 3 years. 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, and updates and reminders will be provided regularly and where changes to legislation, guidance or the School's/Trust's processes make it necessary. Other training resources are available on Foldr.

19. Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the Trust's overall compliance with data protection law, The Head of Trust Services has responsibility for monitoring and reviewing this policy, in conjunction with the DPO and Headteachers are responsible for the day to day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the Trust'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.

20. Complaints

The Trust is always seeking to implement best practice and strives for the highest standards. The Trust operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The Trust's complaints policy may be found on its website.

There is a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the School/Trust or via the Trust's DPO.

The ICO is contactable at:

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
Telephone: 0303 123 1113.

21. Legislation and Guidance

This policy takes into account the following:

- The United Kingdom General Data Protection Regulation (UKGDPR)
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Protection of biometric information of children in schools and colleges – DfE March 2018
- Information Sharing – Advice for Practitioners – DfE July 2018.

22. Links with Other Policies

This Data Protection Policy is linked to the following:

- Trust Freedom of Information Policy
- Trust Records Management Policy and Guidelines
- School Bring your own device Policy
- School Privacy Notices (templates provided)
- School Safeguarding Policy
- School Acceptable Usage Policies
- School E-Safety/Online Safety Policy
- School Consent / Permissions Form (templates provided)
- Admissions Form
- GDPR Contractor Agreement and Third Party Questionnaire

Appendix 1 – Examples of Special Category Data that we process

Examples of where we may process special category data include :

- Pupil health/disability data and information concerning their racial / ethnic origin in admissions records and in pupil records / trip packs
- School census information
- Attendance records
- Biometric data i.e., 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 and 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 which may be found on our website.

Appendix 2 – Subject Access Request Procedure (SAR)

The Trust shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (i-west) and using their School SAR Guidance.

1. Requests for information may be made verbally or in writing; which includes email, and be addressed to the Data Protection Officer, Lighthouse Schools Partnership, c/o St Mary's Road, Portishead, Bristol, BS20 7QR, (DPO@lsp.org.uk). Requesters making a verbal request will be encouraged to confirm their request in writing. If staff receive a SAR, they must immediately forward it to the DPO email address (dpo@lsp.org.uk). If the initial request does not clearly identify the information required, then further enquiries will be made.

2. Ascertain whether the requester has a right to access the information and capacity. The Trust will not disclose information if an exemption applies, for example where it:
    a. Might cause serious harm to the physical or mental health of the pupil or another individual
    b. Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
    c. Is contained in adoption or parental order records
    d. Is given to a court in proceedings concerning the child

    A request may be deemed manifestly unfounded or excessive for example if it is repetitive (i.e. it repeats the substance of previous requests and a reasonable interval has not elapsed between requests), or overlaps with other requests
    If the Trust refuses a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

3. Obtain proof of identity (once this step has been completed the clock can start). Unless the identity of the requester is obvious (for example where there is an ongoing relationship with a known requester) then the identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity should be reasonable and can be established by requesting production of:
    a. passport
    b. driving licence
    c. utility bills with the current address
    d. Birth / Marriage certificate
    e. P45/P60
    f. Credit Card or Mortgage statement

    This list is not exhaustive. Copies of identification documentation will not be retained but a record made of its production.

4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost (i.e. you may not charge for time taken to deal with the request).

6. Use its Record of Processing Activities 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 data sources including staff emails where it is necessary to do so in accordance with this policy and the ICO's 'Employment Practices Code'.

8. If (6) identifies third parties who process it, then engage with them to release the data to the school.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer (i-west), and their School SAR Guidance.

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.

LIGHTHOUSE
SCHOOLS PARTNERSHIP

Appendix 3 - Personal Data Breach Procedure

In the event of a suspected personal data breach, the following procedure should be followed:

1. The Data Lead at the school/Trust will try to contain the breach and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.
2. Report the potential breach, as soon as possible, to the Data Protection Lead and/or Headteacher of the school in which the potential breach has occurred.
3. The Data Protection Lead and/or Headteacher of the school will then report to the potential breach to the Trust using the email address DPO@lsp.org.uk. This will also be shared with the Trust's Data Protection Officer (DPO), provided by i-west.
4. The Headteacher of the school in which the potential breach has occurred will complete an incident report. The incident report will document the facts relating to the potential breach, its effects and any initial remedial action to be taken. The completed incident report should be shared with the Trust via DPO@lsp.org.uk. A template incident report can be found in Appendix 4.
5. With the information in the incident report, the DPO will ascertain if a breach of personal data has occurred. A personal data breach is one which, if not addressed in an appropriate and timely manner, may result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the individual concerned.
6. If it is likely that there will be a risk to people's rights and freedoms as a result of the breach then the DPO will report the breach to the Information Commissioner (ICO) within 72 hours. In these cases, the Data Lead at the school/Trust will also inform those concerned directly and without undue delay.
7. The Trust will investigate every breach of personal data to identify whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.
8. Any changes to procedures, advice or additional training requirements will be shared with leaders and staff in the Trust as appropriate.
9. Any facts relating to the breach, its effects and the remedial action taken will be documented by school/Trust in accordance with the UKGDPR Article 33(5) and with our obligation to comply with the accountability principle.

LIGHTHOUSE
SCHOOLS PARTNERSHIP

Appendix 4 - 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 LSP's 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 school's data lead and/or the Headteacher

The incident may require additional input and support from other organisations such as ICT, the school's Data Protection Lead, The LSP's 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? 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: DPO@lsp.org.uk

LIGHTHOUSE
SCHOOLS PARTNERSHIP

Appendix 5 – GDPR Walkabout Checklist

Good data protection practices should be ingrained into the ethos of the 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.

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

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.