Staff Data Privacy Policy

The Bay Learning Trust
The Lodge
Ripley St Thomas
Ashton Road
Lancaster
LA1 4RR

t 01524 581872
e admin@baylearningtrust.com
website baylearningtrust.com

Document Control

This document has been approved for operation within:	**All Trust Establishments**
Date effective from	**October 2021**
Date of next review	**October 2023**
Review period	**2 Years**
Status	**Statutory**
Owner	**The Bay Learning Trust**
Version	

1 INTRODUCTION

1.1 This Data Privacy Policy contains important information about how and why The Bay Learning Trust (**Trust**) collects, processes, stores and shares Personal Data belonging to Trust employees, workers, directors, members, governors and third parties e.g. pupils and parents (Third Party Data).

1.2 The focus of this policy is on the Trust's duties and responsibilities in respect of the Personal Data of Trust employees and workers (**Staff**), and directors, members, governors, and the duties and responsibilities Trust Staff have to Process the Personal Data of Trust Staff and Third Party Data in accordance with Trust policies, procedures and the law.

1.3 This Data Privacy Policy should be read in conjunction with the Trust's:

- GDPR & Pupil Records Data Privacy Policy;
- Privacy Notice for School Workforce;
- Records Retention Policy;
- Disciplinary Policy (Staff).

2 DATA PRIVACY: THE BASICS

2.1 In legal terms, this process of collecting and processing Personal Data means that the Bay Learning Trust is referred to as a Controller (**Controller**).

2.2 Any external person or organisation that Processes Personal Data on the Trust's behalf and on the Trust's instructions (e.g. a payroll provider or insurance company) is referred to as a Data Processor (**Processor**).

2.2 Any activity that involves the use of Personal Data is referred to as Processing (**Processing/Process/Processes**). It includes:

- Obtaining, recording or holding Personal Data;
- Carrying out any operation or set of operations on Personal Data (e.g. organising, amending, retrieving, using, disclosing, erasing or destroying it); and
- Transmitting or transferring Personal Data to third parties.

2.3 Personal Data is any information identifying or relating to an identifiable Data Subject (**Personal Data**). A person is considered to be a Data Subject if he or she is a living individual that can be identified (directly or indirectly) from the Personal Data (**Data Subject**). Personal Data includes some Special Category Data and Criminal Conviction Data.

2.4 The following table gives a non-exhaustive list of examples of what is included and excluded from these definitions:

Personal Data		Excluded / Not Personal Data
Personal Data	**Special Category & Criminal Conviction Data (formerly called Sensitive Personal Data)**	
• Name • Address • Telephone number • Date of birth • Gender • Qualifications • Opinions about an individual's actions or behaviour (e.g. references, Staff appraisals, disciplinary records) • Location data	• Racial or ethnic origin • Political opinions • Religious or similar beliefs • Trade union membership • Physical or mental health conditions (e.g. sick notes, medical reports) • Sexual life • Sexual orientation • Biometric or genetic data • Criminal offences and convictions (e.g. DBS checks)	• Anonymous data • Data that has had the individual's identity permanently removed (e.g. statistical information about the gender breakdown of our Staff from whom individuals cannot be identified)

2.5 **The rights as a Data Subject**

Each Data Subject has legal rights designed to protect the privacy of their Personal Data. Each person is a Data Subject (with regard to their own Personal Data). This Staff Data Privacy Policy explains more about the rights as a Data Subject and the responsibilities in relation to Processing Personal Data of Third Parties.

2.6 **Third Party Data: The Trusts's duties and responsibilities**

2.6.1 To the extent that the Trust is involved in the Processing of Personal Data, the Trust will have legal duties and responsibilities to Process the Personal Data of others in accordance with this Data Privacy Policy and the law governing data privacy, including the GDPR (see "The Trust's commitment to complying with data protection procedures" below).

2.6.2 If a member of the Trust's role involves regular Processing of Personal Data, or might reasonably bring them into contact with Personal Data, that person will receive training on the Trust's data privacy policies and procedures as part of their induction and this will be refreshed at regular intervals thereafter (see "Staff Training" below).

2.7 **Data privacy: The Trust's collective responsibility**

The Bay Learning Trust takes its legal obligations and responsibilities regarding data privacy very seriously. The Trust expects all of their Staff to treat any Personal Data they may come into contact with (whether it is part of their role to handle such data or not) sensitively and in accordance with the Trust's data privacy policies and procedures. The Trust is reminded that any breach of this policy, the Trust's data privacy procedures, or the law governing data privacy, may result in disciplinary action.

3 OUR COMMITMENT TO COMPLYING WITH THE DATA PROTECTION PRINCIPLES

3.1 Personal Data must be Processed in compliance with the Data Protection Principles (**DPP**) relating to the Processing of Personal Data (as set out in the General Data Protection Regulation (EU 2016/679) (**GDPR**). The DPP require Personal Data to be:

Data Protection Principle (DPP)	Details
Processed lawfully, fairly and in a transparent manner	Personal Data must be Processed on the basis of one or more of the conditions specified in the GDPR.
Collected only for specified, explicit and legitimate Purposes.	If the Trust collects Personal Data directly from Data Subjects, the Trust will inform the Data Subject about: • The Purpose(s) for which the Trust intends to Process their Personal data; • The third parties (if any) with which the Trust will share, or to which the Trust will disclose, their Personal Data; and • Their rights as a Data Subject (e.g. to access and rectify their Personal Data). Personal Data must not be Processed in any manner incompatible with those original purposes.
Adequate, relevant and limited to what is necessary in relation to the Purposes for which it is Processed.	The Trust will only collect Personal Data to the extent that it is required for the specific Purpose notified to the Data Subject.
Accurate and where necessary kept up to date	The Trust will ensure that Personal Data the Trust holds is accurate and kept up to date. The Trust will check the accuracy of

	any Personal Data at the point of collection and at regular intervals afterwards. Data subjects are required to keep us informed of any changes to their Personal Data so that the Trust can keep the Trust's records accurate. The Trust will take all reasonable steps to, without delay, destroy or amend inaccurate or out-of-date Personal Data.
Not kept in a form which permits identification of a Data Subject for longer than is necessary for the Purposes for which the data is Processed.	The Trust follows current data retention guidelines and have procedures for the deletion and destruction of data in accordance with those guidelines.
Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage.	The Trust will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, personal data. The Trust have put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal data will only be transferred to a Data Processor if they agree to comply with those procedures and policies, or if they also put in place adequate security measures.
Made available to the Data Subject on request and that Data Subjects are allowed to exercise certain rights in relation to their Personal Data	The Trust will Process all Personal Data in line with Data Subjects' rights, in particular their right to: • Request access to any Personal Data held about them; • Prevent the Processing of their Personal Data for direct-marketing Purposes; • Ask to have inaccurate Personal Data amended; and • Prevent Processing that is likely to cause damage or distress to themselves or anyone else.
Not transferred to people/organisations situated in countries without adequate protection	The Trust may only transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), provided

	that one of the following conditions applies: • The country ensures an adequate level of protection for the Data Subjects' rights and freedoms; • The Data Subject has given consent; • The transfer is necessary for one of the conditions set out in the GDPR (e.g. for the performance of a contract between the Trust and the Data Subject, or to protect the vital interests of the Data Subject); • The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or • The transfer is authorised by the Information Commissioner where the Trust have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

4 CONDITIONS FOR PROCESSING

4.1 To be Processed lawfully, Personal Data must be Processed on the basis of one or more of the Conditions specified in the GDPR (**Condition(s)**). The most common Conditions the Trust relies on to Process Personal Data are:

Conditions for Processing which we commonly rely on	
Personal Data	**Special Category Personal Data & Criminal Convictions Data (formerly called Sensitive Personal Data)**
• The Data Subject has given his consent to the Processing for one or more specific Purposes; • Processing is necessary for entering or performing a contract with the Data Subject;	• The Data Subject has given explicit consent to the processing for one or more specific Purposes; • Processing is necessary for the Purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law so far as it is authorised by

• Processing is necessary for compliance with a legal obligation to which the Controller is subject; • Processing is necessary to protect the vital interests of the Data Subject; or • Processing is necessary for the Purposes of legitimate interests pursued by the data controller or by a third party.	Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; • Processing is necessary to protect the vital interests of the Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent; • Processing is necessary for the establishment, exercise or defence of legal claims; or • 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.

4.2 However, the Trust may in some circumstances rely on other Conditions set out in the GDPR or Data Protection Act 2018 to justify the Processing of Personal Data or Special Category Personal Data.

4.3 Personal Data must only be collected or Processed for specified, explicit and legitimate Purposes. The Trust will establish and record the Condition for Processing each time Processing of Personal Data occurs.

4.4 Staff are forbidden from Processing Personal Data for Purposes which go beyond or are incompatible with the original Purposes specified to the Data Subject in the transparency information provided to them (see "Transparency: notifying Data Subjects" below).

4.5 **Consent**

4.5.1 Consent (**Consent**) is one of the many Conditions upon which the Processing of Personal Data can be based. However, in lots of circumstances the Trust will rely on other Conditions to process Personal Data. For example, the Trust do not routinely rely on Consent as a Condition to justify the Processing the Personal Data of our Staff. This is explained further in your personal Privacy Notice for School Workforce.

4.5.2 Key points to note about relying on Consent as a Condition for Processing:

- Consent requires affirmative action; silence, pre-ticked boxes or inactivity should not be considered to be consent;
- Consent must be kept separate from other terms and conditions, so that it is clear and unambiguous;
- Use clear and plain language when explaining Consent;
- Consent must be specific and informed, meaning it should be clear to the Data Subject what it is they are consenting to and how and why their Personal Data will be Processed;
- The Data Subject must be free to refuse to give their Consent to the Processing;
- If Consent is relied upon, the Data Subject must be easily able to withdraw their Consent to Processing at any time and withdrawal must be promptly honoured;
- Consent should be refreshed if Personal Data will be Processed for a different and incompatible Purpose to that disclosed when the Data Subject first consented;
- Consent should not be relied upon as a Condition for Processing where there is an imbalance of power between the Trust and the Data Subject; and
- Records should be kept of any Consent received (what consent was given, when and how it was obtained).

5 WHAT RIGHTS DO DATA SUBJECTS HAVE?

5.1 Data Subjects have rights when it comes to how the Trust handles their Personal Data. Some of these rights are dependent on the nature and purposes of the processing. In summary, these include rights to:

- Withdraw consent to Processing at any time where the Trust have relied on consent to conduct the Processing (see above "Consent");
- Receive certain information about the Trust's Processing activities (see "Transparency: notifying Data Subjects" below);
- Request access to the Personal Data that the Trust holds on them (see "Subject Access Requests" below);
- Prevent the Trust's use of their Personal Data for direct marketing purposes;
- Ask the Trust to erase Personal Data if it is no longer necessary in relation to the Purposes for which it was collected or Processed, or to rectify inaccurate data or to complete incomplete data;
- Restrict Processing in specific circumstances;

- Challenge Processing which has been justified on the basis of the Trust's legitimate interests or in the public interest;
- Request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- Prevent Processing that is likely to cause damage or distress to them or anyone else;
- Be notified of any Personal Data Breach which is likely to result in a high risk to their rights and freedoms;
- Make a complaint to the Information Commissioner; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

5.2 Staff who wish to exercise a right on their own behalf or who receive a written request from a Data Subject who wishes to exercise any of their GDPR or data privacy rights (for example, requesting the rectification or deletion of their Personal Data) should contact the Trust's Data Protection Officer immediately (contact details are on page 14).

5.3 **Subject Access Requests**

5.3.1 Data Subjects may make a formal written request for details of the Personal Data the Trust holds about them (**Subject Access Request**). The GDPR requires the Trust to deal with Subject Access Requests within strict time-limits. Therefore, Staff who receive a written request for access to Personal Data (whether or not the request specifies that it is a Subject Access Request) should forward it to the Trust's Data Protection Officer immediately.

5.3.2 When receiving telephone enquiries, the Trust will only disclose Personal Data the Trust holds on the Trust's systems if the Trust checks the caller's identity to make sure that information is only given to a person who is entitled to it. If the Trust are not sure about the caller's identity, or if their identity cannot be checked, the Trust will ask that the caller put their request in writing.

6 TRANSPARENCY: NOTIFYING DATA SUBJECTS

6.1 The GDPR requires Controllers to provide clear, detailed and specific information to Data Subjects about the Processing of the Personal Data. Such information must be provided through appropriate privacy notices. The Trust's Privacy Notice for School Workforce sets out the information about how the Trust Processes Personal Data. It

will be reviewed annually to ensure the Trust are as transparent as possible about the Personal Data the Trust Processes.

6.2 The GDPR (and the accompanying guidance) is very specific about the language used in any privacy notices. To ensure compliance with the GDPR, the Data Protection Officer must be involved in the drafting of any privacy notices.

7 PURPOSE LIMITATION

7.1 Personal Data must be collected only for specified, explicit and legitimate Purposes (**Purposes**) and must not be further Processed in any manner incompatible with those Purposes. This means that the Trust cannot use Personal Data for new, different or incompatible Purposes from that disclosed when it was first obtained unless the Trust have informed the Data Subject of the new Purposes, and (if this is the Condition relied upon to Process their Personal Data) they have given their Consent. To ensure compliance with this Purpose limitation requirement:

- The Trust will establish and record the Purposes for Processing each time Personal Data is collected;
- Staff who are responsible for collecting or Processing Personal Data must ensure on each occasion that the Purposes for doing so are not incompatible with the original specified Purposes. If the Purposes are incompatible, the Data Subject must be notified of the new Purposes as soon as possible.

7.2 The Trust's Staff are reminded that Processing Personal Data for Purposes which are incompatible with the Purposes for which the Personal Data was obtained is considered a serious breach of this Data Privacy Policy and may result in disciplinary action.

8 DATA MINIMISATION

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the Purposes for which it is Processed. This means that the Trust:

- May only collect or Process Personal Data when performing job duties requires it;
- Cannot Process Personal Data for any reason unrelated to job duties;
- Must not collect excessive Personal Data, which is not relevant for the specified Purposes;
- Must ensure that when any Personal Data is no longer needed for the specified Purposes, it is deleted or anonymised in accordance with the Trust's Records Retention Policy.

9 DATA ACCURACY

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. To the extent that the job requires the Trust to collect or Process Personal Data, this means that the Trust:

- Must ensure that the Personal Data the Trust uses and hold is accurate, complete, kept up to date and relevant to the purpose for which the Trust collected it;
- Must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards; and
- Must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10 STORAGE LIMITATION

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the Purposes for which the data is Processed. The Trust (and to the extent that duties involve the Processing of Personal Data, employees, workers, directors, members and governors) must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate Purposes for which the Trust originally collected it.

10.2 The Bay Learning Trust's Data Retention Policy is designed to ensure Personal Data is deleted after a reasonable time, unless a law requires such Personal Data to be kept for a minimum time. The Records Retention Policy is available from the Policies section of the Trust's website or is available in hard copy format upon request.

10.3 The Trust (and to the extent that duties involve the Processing of Personal Data, employees, workers, directors, members and governors) will take all reasonable steps to destroy or erase from the Trust's systems all Personal Data that the Trust no longer require in accordance with the Trust's Records Retention Policy.

11 DATA SECURITY

11.1 The Trust will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. The Trust have procedures and technologies in place which are designed to maintain the security of Personal Data from the point of collection to the point of destruction. In summary, this means that the Trust and the Trust's Staff must ensure that:

- Only people who are authorised to use the Personal Data can access it;

- Steps are taken to ensure that people who are authorised to access Personal Data are not accessing or Processing Personal Data for reasons which are unrelated to their job role;
- Steps are taken to verify the identity of a Data Subject before discussing their Personal Data with them;
- Personal Data is stored on the Trust's central computer or cloud systems instead of individual PCs, laptops, tablet devices, mobile telephones etc;
- Computers and laptops are not left unattended without locking their screens via password controls to prevent unauthorised access;
- Personal Data is not carried off-site, save on permitted storage devices which are encrypted and password protected or when it is legally necessary to do so. Where Personal Data needs to be carried off-site in paper form, Staff must obtain permission from their Principal or the CEO.
- Personal Data Breaches, or circumstances which might reasonably lead to a Personal Data Breach, are promptly reported; and
- The Trust's security procedures (e.g. ensuring offices are locked when not in use and shredders / confidential shredding services are used for Personal Data) are followed.

11.2 The Trust's Staff are reminded that any breach of our data security procedures is considered a serious breach of this Data Privacy Policy and may result in disciplinary action.

11.3 **Staff Training**

11.3.1 As part of the Trust's commitment to data security, all Staff will receive training on the Trust's data privacy policies and procedures as part of their induction and this will be refreshed at regular intervals thereafter.

12 **MANDATORY DATA BREACH REPORTING**

12.1 Under the GDPR, the Trust has certain obligations to mandatorily report Personal Data Breaches. A Personal Data Breach (**Personal Data Breach**) is 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.

12.2 There are two levels of mandatory reporting obligation, which depend upon the level of risk arising from the Personal Data Breach:

Mandatory Reporting Obligation	Details
Report to Information Commissioner must be made ASAP (at latest within 72 hours of becoming aware of the Personal Data Breach).	If the Personal Data Breach is likely to result in **a risk** to Data Subject's rights and freedoms. Examples: • Report: – e-mailing details of an SEN pupil's assessments to the wrong external e-mail address; – a ransomware attack which results in all personal data being encrypted and no back-ups are available. • Do not report: – loss of a staff telephone list; – loss of a securely encrypted mobile device, provided the encryption key remains within the Trust's secure possession and this is not the sole copy of the Personal Data.
Notify Data Subject "without undue delay" and "as soon as reasonably feasible".	If a Personal Data Breach poses a **high risk** to a Data Subject then it must be directly reported to them as well as the Information Commissioner unless an exception applies. High risk situations are likely to include the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation or financial loss. Examples of high risk Personal Data Breaches: • A cyber-attack leads to Personal Data being exfiltrated from our server; • The Trust suffers a ransomware attack which results in all Personal Data being encrypted. No back-ups are available and the data cannot be restored; and There are some limited exceptions to the mandatory requirement to report a Personal Data Breach to the Data Subject.

12.3 Failure to make the relevant mandatory Personal Data Breach report may lead to a financial sanction against the Trust.

12.4 It is the responsibility of all Staff to **immediately** report any Personal Data Breach which comes to their attention (whether it involves that member of Staff, whether subordinate or senior to employees, workers, directors, members and governors), or

circumstances which might reasonably be interpreted as a Personal Data Breach, or which could lead to a Personal Data Breach to the **Data Protection Officer**.

13 DATA PROTECTION OFFICER

13.1 The Trust has appointed a Data Protection Officer for GDPR purposes, who has overall responsibility for the Trust's policies and procedures relating to data privacy. The Data Protection Officer should be the first point of contact in the following situations:

- If a member of staff has any concerns, or requires clarification, about their or the Bay Learning Trust's obligations regarding data privacy;
- If staff have any feedback or suggestions about how the Trust can improve its data privacy and/or data security procedures;
- If staff receive a request from a Data Subject seeking to:
  - Access their Personal Data (see "Subject Access Requests" above); or
  - Exercise any of their other rights as a Data Subject (see "What rights do Data Subject's have?" above), such as to withdraw their Consent to Processing;
- If the Trust becomes aware of any member of Staff:
  - Abusing their role to access Personal Data for non-permitted reasons;
  - Processing Personal Data in a manner which is inconsistent with this Data Privacy Policy;
  - Committing a breach of our Data Retention Policy.
- If employees, workers, directors, members and governors, or any other member of Staff are involved in a Personal Data Breach, or circumstances which might reasonably be interpreted as a Personal Data Breach, or which could lead to a Personal Data Breach (see "Mandatory Data Breach Reporting" above).

13.2 The Trust's Data Protection Officer is Gavin Gomersall. His contact details are:

Data Protection Officer
The Bay Learning Trust
The Lodge
Ripley St Thomas
Ashton Road
LA1 4RR
Email: gomersallg@baylearningtrust.com
Phone: 01524 581865