



Data Protection Policy

December 2025

Reviewed by Executive Team:	November 2025
Endorsed by [committee]:	N/A
Approved by Board:	9 December 2025
Next review	Autumn 2026

1. Introduction

- 1.1. Horsham Learning Alliance (the Trust) is committed to all aspects of data protection and takes seriously its duties and the duties of its employees. This policy set outs how the organisation deals with personal data, including personnel files, data subject access requests, and employees' obligations in relation to personal data.
- 1.2. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the Trust.

The Trust, and the College/schools within it, collects, uses, and stores personal data about its students, parents/carers, employees, Members, Trustees and Local Governors, suppliers, visitors, and volunteers. The Trust recognises that having controls around the collection, use, retention, and destruction of personal data is important to comply with the obligations under Data Protection Laws, and particularly its obligations under Article 5 of GDPR.

The Trust has implemented this Data Protection Policy to ensure all College/school staff, including volunteers and Members, Trustees, Local Governors are aware of what they must do to ensure the correct and lawful treatment of personal data.

- 1.3. If you have any queries concerning this policy, please contact a member of the Data Protection Team, as below:

Role	Organisation	Contact
Trust Data Protection Officer (DPO)	Horsham Learning Alliance	DPO@hla.education
Data Protection Lead	The College of Richard Collyer	DataProtection@collyers.ac.uk
Data Protection Lead	The Forest School	dp@theforestschool.net

2. Legislative Framework

- 2.1. The following legislative framework informs the Trust's undertaking to protect the personal data of all stakeholders and comply with all legislative requirements:
 - The General Data Protection Regulation 2018
 - Data Protection Act 2018
 - Information Commissioners Office (ICO): ICO Guide to Data Protection
 - Freedom of Information Act 2000

3. Scope

- 3.1. This policy sets out the basis on which the Trust will collect, use, transfer and store personal data.
- 3.2. The Data Protection Act 2018 regulates all activities that are involved with the "processing" of personal data. The definition of processing is very wide and therefore

this policy assumes that everything that the Trust, and the College/schools within the Trust, does with personal data is processing.

- 3.3. Processing, in relation to information or data, means obtaining, recording or holding the information or data or conducting any operation or set of operations on the information or data, including:
- Organisation, adaptation or alteration of the information or data
 - Retrieval, consultation or use of the information or data
 - Disclosure of the information or data by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or data

3.4 This policy applies to all personnel who collect and/or use personal data within the organisation.

3.5 This policy applies to all personal data which is stored electronically, in paper form, or otherwise.

4. Definitions

4.1. Data Controller

A Data Controller is any individual or organisation that determines the purposes and means of processing personal data. This means they have overall control and decide how, why, and what data is processed, and for how long. The Data Controller holds the primary responsibility for compliance with Data Protection Laws. Horsham Learning Alliance is the Data Controller.

4.2. Data Processor

A Data Processor is a third party that processes personal data on behalf of a Data Controller. A Data Processor does not determine the purposes or means of the processing but acts on the authority and instructions of the Data Controller. This is usually because of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of personal data. Examples include where software support for a system, which contains personal data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

4.3. Data Subject

A Data Subject is the identified or identifiable individual whose personal data is held or processed.

4.4. Data Protection Officer

The Data Protection Officer is responsible for ensuring an organisation's compliance with data protection laws.

4.5. Data Protection Laws

The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

4.6. Information Commissioner's Office (ICO)

The UK's independent authority responsible for upholding information rights, including data protection and privacy.

4.7. Individuals

Living individuals who can be identified, directly or indirectly, from information that the Trust holds. For example, an individual could be identified directly by name, or indirectly by gender, job role, and office location if you can use this information to work out who they are. Individuals include employees, students, parents/carers, visitors, potential students, partnerships, and sole traders.

4.8. Personal Data

Any information about an Individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and more sensitive types of data such as trade union membership, genetic data, and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

4.9. Special Categories of Personal Data

Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4.10 Personnel

Any employee or contractor who has been authorised to access any of the organisation's personal data and will include employees, consultants, contractors, and temporary personnel.

5. Aims

- 5.1. The Trust aims to ensure that all personal data collected about staff, students, parents/carers, trustees, governors, visitors and other individuals is collected, stored, and processed in accordance with UK data protection law.

5.2. The Trust aims to ensure that the following data protection principles are followed in the handling of personal data.

5.2.1 Data is processed in a way that is lawful, fair and transparent.

5.2.2 Data is collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.2.3 Data collected is adequate, relevant, and limited to what is necessary for the purposes for which it is being processed.

5.2.4 Personal data held is accurate and kept up to date.

5.2.5 Data is not kept in a form that identifies the data subject longer than is necessary for the purposes for which it is being processed.

5.2.6 Data is processed in a manner that ensures appropriate security, protecting against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.2.7 The Trust, as Data Controller, will be responsible for and demonstrate compliance with the principles of UK GDPR.

6. Use of Data

6.1. Personal Data

The Trust will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

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

6.2. Special Categories

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- a) the individual (or their parent/carer when appropriate in the case of a school student) has given explicit consent.
- b) the data needs to be processed to perform or exercise obligations or rights in relation to employment, social security, or social protection law.
- c) the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- d) the data has already been made manifestly public by the individual.
- e) the data needs to be processed for the establishment, exercise, or defence of legal claims.
- f) the data needs to be processed for reasons of substantial public interest as defined in legislation.
- g) the data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- h) the data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- i) the data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

6.3. Criminal Offence Data

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- a) the individual (or their parent/carer when appropriate in the case of a school student) has given consent.
- b) the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
- c) the data has already been made manifestly public by the individual.
- d) the data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of legal rights.
- e) the data needs to be processed for reasons of substantial public interest as defined in legislation.

6.4. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not expect or use personal data in ways which have unjustified adverse effects on them.

6.5. Consent may be given or withdrawn by any person aged 13 or over, and where this is the case, separate consent is not required from parents/carers.

7. Limitation, minimisation, and accuracy

- 7.1. We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- 7.2. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
- 7.3. Staff must only process personal data where it is necessary to do their jobs.
- 7.4. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- 7.5. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

8. Sharing personal data

- 8.1. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:
 - there is an issue with a student or parent/carer that puts the safety of our staff or another individual at risk.
 - we need to consult with other agencies – we will seek consent as necessary before doing this.
 - our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
 - only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law.
 - establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
 - only share data that the supplier or contractor needs to conduct their service.
- 8.2. We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- 8.3. We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our students or staff.
- 8.4. Where we transfer personal data internationally, we will do so in accordance with UK data protection law.
- 8.5. The Trust including the College/schools have a legal duty under the Children Act (2004) to inform local authorities where a child's welfare is at risk. Where the Data

Subject is under 18, the Trust, College/school does not require consent to inform the relevant Local Authority where it has concerns. However, wherever possible, the Data Subject will be properly informed of the process, according to the relevant Safeguarding Policy.

9. Subject Consent

- 9.1. In many cases, the Trust can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College/schools processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.
- 9.2. Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The Trust has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The Trust also has a duty of care to all staff and students and must, therefore, make sure that employees and those who use the College/schools facilities do not pose a threat or danger to other users. Where an enhanced Disclosure and Barring check is required, consent will be requested and information collected, stored, and processed in accordance with the Data Protection Act 2018. A refusal to sign such a form can result in the offer of a position, paid or voluntary (staff including governors and volunteers) or course (students) being withdrawn.
- 9.3. The College/schools will also ask for information about health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The Trust will only use the information in the protection of the health and safety of the individual but will need consent to process for example in the event of a medical emergency.
- 9.4. All prospective staff (including volunteers and governors) and students will be asked to sign a 'Consent to Process' form, regarding types of information when an offer of a position or a course place is made.
- 9.5. Prospective staff (including volunteers, trustees, and governors) will be asked to sign a HR data form to give permission for specified personal data to be shared with authorised staff. The staff employment contract gives specific consent to the Trust retaining computer and paper-based records.

10. Processing Sensitive Information

- 10.1. Occasionally it is necessary to process information about a person's health, criminal convictions, race, gender, and family details. This may be to ensure that the College/schools is a safe place for everyone, or to operate other Trust policies, such as the Equality and Diversity Policy. As this information is considered sensitive and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the

College/schools to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the HR Director or Student Services.

11. Subject access requests

11.1. Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for, or if this is not possible, the criteria used to determine this period
- where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing
- the right to lodge a complaint with the ICO or another supervisory authority
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- the safeguards provided if the data is being transferred internationally

11.2. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- name of individual
- correspondence address
- contact number and email address
- details of the information requested

11.3. If staff receive a subject access request in any form, they must immediately forward it to the DPO.

11.4. Subject access requests – children

Personal data about a child belongs to that child, and not the child's parents/carers. For a parent/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.

11.5. Children below the age of 13 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/carers of students in the Trust may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

11.6. Children aged 13 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/carers of students at our Trust may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

11.7. When responding to requests, we:

- may ask the individual to provide forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- will provide the information free of charge
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous, or falls within the summer holiday period when staffing is limited. We will inform the individual of this within 1 month and explain why the extension is necessary

11.8. We may not disclose information for a variety of reasons, such as if it:

- might cause serious harm to the physical or mental health of the student or another individual
- would reveal that the student is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the student's best interests
- would include another person's personal data that we can't reasonably anonymise, and we do not have the other person's consent, and it would be unreasonable to proceed without it
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

11.9. If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision. When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO, or they can seek to enforce their subject access right through the courts.

12. Data Security

12.1. The Trust takes information security very seriously and has security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. The Trust has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

13. Data Retention

- 13.1. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The Trust will keep some forms of information for longer than others, as set out in the Data Retention Policy.
- 13.2. Due to storage considerations, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general, personal data relating to students will be kept for a minimum of seven years after the student's final course leaving date. This will include:
- Name and address
 - Academic achievements, including marks for coursework
 - Copies of any reference written
 - The Learning Agreement
- 13.3. The Trust will keep information about staff for a minimum of seven years after a member of staff leaves employment.

14. Data Breach

- 14.1. Whilst the Trust takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of personal data. If this happens there will be a Personal Data Breach and the Trust's Data Protection Officer team must be notified.
- 14.2. A personal data breach is defined very broadly and is effectively any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of personal data.
- 14.3. There are three main types of personal data breach which are as follows:
- 14.3.1 Confidentiality breach** – where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a staff member is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people “blagging” access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- 14.3.2 Availability breach** – where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and
- 14.3.3 Integrity breach** – where there is an unauthorised or accidental alteration of Personal Data.

- 14.4. In the event of a data breach, this must be reported immediately to the College/schools Data Lead, or the Trust DPO. The Data Lead will manage the internal investigation process, including notifying the individuals affected by the data breach and ensuring the person responsible for the data breach receives additional training.
- 14.5. The Trust DPO will assess the impact, how it may be rectified and documented, consider any training required for employees, and will report to the ICO, as appropriate.

15. Right of erasure

- 15.1 This is a limited right for individuals to request the erasure of personal data concerning them where:
- the use of the Personal Data is no longer necessary;
 - their consent is withdrawn and there is no other legal ground for the processing;
 - the individual objects to the processing and there are no overriding legitimate grounds for the processing;
 - the Personal Data has been unlawfully processed; and
 - the Personal Data has to be erased for compliance with a legal obligation.

In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

16. CCTV, Body Worn Cameras (BWC) and Biometrics

- 16.1. The CCTV and Body Worn Cameras Code of Practice is to regulate the management, operation and use of the CCTV and Body Worn Cameras at the College/schools and is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements of the Data Protection Act, the Commissioner's Code of Practice and the Freedom of Information Act 2000.
- 16.2. Information about the use of biometrics can be found in the Biometrics Policy.

17. Examination Marks

- 17.1. Students will be entitled to information about their examination marks; however, this may take longer than other information to provide. The College/schools may withhold certificates or references if the full course fee has not been paid (when applicable), there are outstanding debts or books, or equipment/materials have not been returned to the College/schools.

18. Responsibilities

18.1. Board of Trustees

The Board of Trustees have overall responsibility for ensuring that the Trust complies with all relevant data protection principles.

18.2. Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, providing technical expertise and guidance to the Executive Principal/Headteacher, reporting data breaches to the ICO, and developing relevant policies and guidelines, as applicable.

18.3. Data Leads

The Data Leads for each College/schools are responsible for investigating data breaches in each location, reporting these to the DPO, and providing relevant training to staff in each location.

18.4. Executive Principal/Headteacher

The Executive Principal/Headteacher will act as the day-to-day representative of the data controller.

18.5. All Staff

All staff are responsible for:

- 18.5.1 Checking that any information that they provide to the Trust in connection with their employment is accurate and up to date
- 18.5.2 Informing the College/schools of any changes to information, which they have provided, for example changes of address
- 18.5.3 Checking the information that the College/schools will send out from time to time, giving details of information kept and processed about staff
- 18.5.4 Informing the Trust of any errors or changes to personal data. The College/schools cannot be held responsible for any errors unless the staff member has informed the College/schools of them
- 18.5.5 When collecting personal data about other people (e.g. about students' coursework, opinions about ability, reference to other academic institutions, or details of personal circumstances), comply with the guidelines for staff on SharePoint
- 18.5.6 Store any personal data safely and only for legitimate purposes, as set out in this policy
- 18.5.7 Not disclose any personal data either orally or in writing or accidentally or otherwise to any unauthorised third party
- 18.5.8 Store sensitive data in a locked filing cabinet, drawer, office or if it is computerised, be password protected or if staff access sensitive data on a personal device, it should be password or PIN protected (e.g. E-mail linked to their smartphone)
- 18.5.9 Never keep sensitive data on portable disc, USB drive or a tablet
- 18.5.10 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by this Trust policy
- 18.5.11 A member of staff, who considers the policy has not been followed in respect of personal data about themselves, should raise the matter with the

designated Data Lead for the College/schools initially. If the matter is not resolved it should be escalated to the DPO for further review

18.5.12 Compliance with the Data Protection legislation is the responsibility of all members of the Trust. Any deliberate breach (including non-disclosure of data loss, paper, phone or tablet) of this policy may lead to disciplinary action being taken, or access to facilities being withdrawn, or even a criminal prosecution. Staff should also note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases

18.5.13 Any questions or concerns about the interpretation or operation of this Policy should be taken up with the designated Data Lead/s

18.6. All College Students

18.6.1 Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of personal details are notified to their tutor who in turn will inform the Registry team.

18.7. All Students

18.7.1 Students who use the College/schools computer facilities may, from time to time, process personal data which will be password protected

18.8. All Parents/Carers of school students

18.8.1 Parents/carers of school-age children must ensure that all personal data provided to the school is accurate and up to date by updating the relevant parent portal of the management information system/s.

19. Monitoring

This policy will be monitored by the DPO and reviewed annually by the Board of Trustees.

20. Related Policies and Procedures

- Appeals Procedure (Staff and Non-Staff)
- CCTV and Body Worn Cameras (BWC) Code of Practice
- Copyright Policy
- Data Retention Policy
- Privacy Notices
- Social Media Policy
- Staff Code of Conduct
- Staff Disciplinary Policy
- Student Behaviour policies
- ICT/Use of Computers Agreements