Data Protection Policy (GDPR)

Policy Version Number:	007	
This policy applies to:	Staff, Students, Parents, Suppliers, Stakeholders	
Related Documents/ Policies:	Academy Privacy Statements Record Retention Policy Freedom of Information Policy IT Security Policy	
Author:	Pamela McIlroy (updated by Corrine Walker)	
Area:	L&M	
Changes made/Reason for Review: Approval required by (please tick):	June 2024 - annual review of policy Nov 2023 - Inclusion of Hathershaw's Biometric Policy A&R ✔ F&R Trust ✔ Rem	
Agreed by/Date: Consultation with/Date: Approved by/Date: Ratified by/Date	DP Committee LJC (if applicable) Committee (A&R) Trust Board	15/5/24 n/a 19/06/2024 16/7/2024
Date of Next Review: Equality Impact Assessment	July 2025 This Policy has been reviewed against equal opportunities legislation with regard to age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity and has no identified adverse impact (direct or indirect) on minority groups	

CONTENTS

1 INTRODUCTION

2 POLICY STATEMENT

- **2.1 Personal Data**
  - **2.1.1 Special Categories of Personal Data/Sensitive Data**
- **2.2 Data Processed by the Trust and its Academies**
  - **2.2.1 Students**
  - **2.2.2 Parents and Emergency Contacts**
  - **2.2.3 Employees**
  - **2.2.4 Other Stakeholders**
- **2.3 Privacy Statements and Consent**
  - **2.3.1 Parental Consent**
- **2.4 Accuracy of Data**
- **2.5 Access to Personal Data (Subject Access Request)**
  - **2.5.1 Data Portability**
  - **2.5.2 The Academy's Rights to Refuse a Request**
- **2.6 Sharing Data**
- **2.7 Automated Decision Making**
- **2.8 Record Retention**
- **2.9 Data Security**
- **2.10 Exemptions**
- **2.11 Privacy Impact Assessments**

3 RESPONSIBILITIES AND COMPLIANCE

- **3.1 The Trust**
- **3.2 The Senior Leadership Team**
- **3.3 Data Protection Officer**
- **3.4 Data Protection Committee**
- **3.5 Staff Responsibilities**
- **3.6 External Data Processors/Third Parties**
- **3.7 Data Breaches**

4 COMPLAINTS AND APPEALS

5 APPENDICES

1 INTRODUCTION

The General Data Protection Regulation (GDPR) is UK legislation which enhances the existing Data Protection Act (1998) in determining how personal data is processed and kept safe and the legal rights individuals have in relation to their own data.

Organisations processing data must comply with the following GDPR principles. Personal Data should be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

Data Controllers are required to show how they comply with the Act by having technical and organisational measures in place, including policies, staff training, documentation and audits. Data Controllers and Processors can receive significant fines for non-compliance.

GDPR also provides the following rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The Pinnacle Learning Trust (the Trust) and the Academies within it (referred to in this document as the Academies) are Data Controllers. The Trust shall take all reasonable steps to implement appropriate technical and organisational measures to demonstrate that it is compliant with the Act and ensure that data is processed in accordance with the legal requirements. Processing is defined as "any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Academies may have contracts with other organisations to process data. These suppliers are Data Processors and they have a legal duty to process data in line with the Act and maintain records of personal data and processing activities. They are responsible for any breach in the data processing. However, the Academy is responsible for ensuring that contracts with Data Processors are compliant with the law and the Trust's Data Protection Policy.

The policy does not form part of any employee's contract of employment and may be amended at any time.

Further information about the GDPR is available from the Information Commissioner's Website

www.ico.org.uk.

2 POLICY STATEMENT

This Policy sets out the basis on which the Trust and its Academies will process any personal data they collect from data subjects, or that is provided to them by data subjects or other sources. It includes the responsibilities of staff within the Trust in complying with GDPR, as well as the rights of individuals whose data is being processed.

The Data Protection Officer (DPO) for the Trust is Corinne Walker. Their responsibilities in this role are detailed in section 3 below. Each Academy will have a nominated person responsible for the compliance of this policy within their Academy. Any questions about the operation of this Policy should be referred to the Data Protection Officer.

2.1 Personal Data

Personal data means "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR applies to both electronic data and manual filing systems. Personal data that has been pseudonymised may still be subject to this Act depending on how difficult it is to attribute the pseudonym to the individual. Personal data covers both facts and opinions about an individual.

2.1.1 Special Categories of Personal Data/Sensitive Data

Special category data is entitled to special protection under the Act, and will only be processed by the Academy with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Special categories include:

- racial or ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

2.2 Data Processed by the Trust and its Academies

During the course of the Trust/Academy's operation it collects, stores and processes personal data about employees, students, parents, suppliers and other third parties. The Trust/Academy will process data which is necessary for compliance with its legal obligation set out by the Department for Education. Other data may be processed in order for the Academy to undertake its day to day functions in terms of employment, education and management. Privacy Statements will inform individuals of how their data is being processed and the legal basis for processing (see section 2.3).

The Academy will consider the following when making decisions to process data or when introducing a new initiative or software, and conduct a DPIA (Data Protection Impact Assessment) where appropriate:

- What information?
- Why is it needed?
- Who will have access to the information?
- Where will it be held?
- How long will it be kept?
- What if consent is not given?
- Who will data be shared with?

Each Academy will keep an up to date Data Asset & Records Retention Map, which will contain the information listed above.

In certain circumstances individuals have the right to restrict processing or to object to processing. In most cases this will not apply to the data processed by the Academy, however if the Academy receives a request from an individual they should consult with the DPO.

2.2.1 Students

Students referred to in this document can be prospective, current or former students.

The Academy will process a wide range of personal data about students as part of its operation. The Academy receives personal data from the individual directly (or, in the case of students under 16, from parents). However in some cases personal data may be supplied by third parties (for example another Academy, or other professionals or authorities working with that individual), or collected from publicly available resources. Additional information will be generated and stored about students during their time at the Academy, such as attendance data, progress, course/timetable information, examination/test results and disciplinary records. Information about what data the Academy processes will be provided in the Privacy Statement. Students and/or their parents are required to sign a declaration to confirm they have read and understood the Privacy Statement on application or enrolment to the Academy.

2.2.2 Parents and Emergency Contacts

Parents are the parents, guardians or carers of prospective, current or former students.

The Academy will record the details of who has parental responsibility for students, plus information regarding parents' names, addresses and contact information in order to meet the requirement to keep parents of students up to the age of 18 informed of their child's progress, attendance, behaviour, etc. The Academy may also contact parents to keep them informed of what is happening at the Academy.

The Academy may also process contact details for Emergency Contacts who do not have parental responsibility.

2.2.3 Employees

Employees refers to applicants, current and former employees, including casual and agency staff, volunteers, Trainee Teachers and subcontracted employees, however the amount and level of data varies depending on the contract with the Trust.

The Trust will collect and process data about employees working for the Trust and its Academies. In most cases this will be provided by the individual, however in some cases personal data may be supplied by third parties (for example a previous employer or other organisation or agency), or collected from publicly available sources. Additional information will be generated and stored about employees during their time at the Academy, such as attendance and performance data. Information about what personal data the Trust processes will be provided in the Privacy Statement which staff are required to sign on application/induction to the Trust.

2.2.4 Other Stakeholders

The Academy will hold data relating to suppliers, subcontractors, and other stakeholders. The Academy will process any such data in accordance with its responsibilities under the Act.

Governors/Trustees will be informed of how the Academy processes information about them in a Privacy Statement.

2.3 Privacy Statements and Consent

The Academy will publish a Privacy Statement for students and employees detailing how it obtains, stores, processes, shares and disposes of personal and sensitive data, and the reason for processing such data. The Privacy Statement will satisfy the individuals' right to be informed. Individuals will be required to agree to the data being used for the purposes identified on the Privacy Statement at the point of application/enrolment to the Academy or Trust. Privacy Statements are available on the Academy and Trust websites. Privacy statements will be reviewed annually.

The processing of any data not contained in the privacy statement will require further information to be provided to individuals and consent, if necessary.

Consent is not required for every piece of data processed as long as the Academy fulfills the legal basis for processing such data. However where consent is required it must be freely given, specific, informed and an unambiguous indication of the individual's wishes. Therefore, the Academy will not assume consent, use opt out clauses or pre-ticked boxes. The Academy will retain copies of consent during the period of processing.

2.3.1 Parental Consent

The Children's Act states that parents have responsibility for decisions about their child's schooling until the age of 18. However, the rights under GDPR are those of the individual to whom the data relate. In most cases where students are under the age of 16, the Academy will rely on parental consent to process data relating to students (if consent is required under the Act) unless, given the nature of the processing in question, and the student's age and understanding, it is more appropriate to rely on the student's consent/agreement.

Students aged 16 and over will be required to give their own consent and will have rights under the Act relating to their own data. However, parents will be required to give consent to the processing of images of their child in relation to their course.

2.4 Accuracy of Data

The Academy will endeavour to ensure that all personal data held in relation to an individual is as up-to date and accurate as possible. Individuals also have a responsibility to notify the Academy of any changes to information held about them. The Academy will regularly make personal data that has been provided by the individual available to those individuals (employees, students or their parents) for checking at least once a year.

An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act). In most cases an employee, a student or their parent who identifies incorrect information about them on the Academy record will simply notify the appropriate department to request that it be amended. The department must keep a record of who made the request, when it was received, when it was amended and by whom (i.e. an audit trail of changes to personal data). However in some circumstances the individual may feel that the matter needs to be brought to the attention of the DPO, in which case they should put this in writing to the DPO.

Under GDPR, the Academy has to correct data within one month of notification, however it is in the Academies' interest to amend the data as soon as is reasonably practical. The DPO will formally respond to any request made to them in writing.

2.5 Access to Personal Data (Subject Access Request)

Individuals have the right under the Act to access personal data about them held by the Academy, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO. Parents can make a Subject Access Request for students aged under 16 and for students 12 and under the request must be made by their parent. The DPO is required to verify the identity of the person making the request.
The Academy will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within statutory time limits (one month). This may be extended to two months if the request or accessing the data is complex, however the individual will be informed of this within the one month timescale.

There will be no charge for providing access to information, unless the request is manifestly unfounded, excessive or repetitive. A charge may be made for providing further copies of information to which the data subject has already been given access. The charge will be based on the actual cost of providing the information and the individual will be advised in advance in writing.

Certain data is exempt from the right of access under the Act; this may include information which identifies other individuals or information which is subject to legal professional privilege.

2.5.1 Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. Requests should be made to the DPO. Where the data can be made available in a commonly used machine readable format, the request will be actioned within one month. There is no charge for providing this data.

2.5.2 The Academy's Rights to Refuse a Request

The Academy reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis :

- Vexatious requests
- Where information held may be required by future legal processes e.g. Child Protection
- The request would lead to inaccurate and misleading information being recorded
- The request has come from an individual who has no rights of access.

Where the Academy decides not to adhere to a request, it will notify the person who requested the reason why the request has been refused; their legal rights of appeal or complaint; their legal rights of referral to the ICO.

2.6 Sharing Data

The Academy may receive requests from third parties to disclose personal data it holds about students, their parents or employees. The Privacy Statements will indicate how and when Academies share data with individuals or organisations outside the Trust. The Academy confirms that it will only disclose information if it is included in the Privacy Statement; the individual has given their explicit consent or one of the specific exemptions under the Act applies. The Trust follows the ICO Data Sharing Code of Practice.

2.7 Automated Decision Making

Individuals have the right to not be subject to a decision based solely on automated processing if it

produces a legal effect or similarly significant effect on the individual. It is unlikely that the Academy will make any decisions based purely on automated processing. If automated processing is used for any decision making, the individual will be informed. In most cases the process will involve some human intervention either at the initial decision making point or in an appeal process.

2.8 Record Retention

The Academy will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, in a secure manner all data which is no longer required in line with the Academies' Data Asset Maps.

The Academy will dispose of its IT equipment in a manner which will protect data security, in line with the Academies' IT Security Policies.

In certain cases, individuals have the right to obtain the erasure of their personal data where the data is no longer necessary in relation to the purpose it was originally collected/processed and its erasure does not conflict with the Trust's legal responsibilities. We recommend that individuals who wish to have their data erased check the guidance on the ICO website and the Trusts' Record Retention Policy before putting their request in writing to the DPO.

2.9 Data Security

The Academy will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of or damage to, personal data. Academy processes will be in place to ensure the security of personal data about individuals, and that members of staff will only have access to personal data relating to students and their parents, or employees, where it is necessary for them to do so.

All staff will be made aware of this policy and their duties under the Act as detailed in section 3 of this policy.

This policy must be read in conjunction with the Academies' IT Policies.

2.10 Exemptions

Certain data is exempted from the provisions of the Act, including the following:

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Academy
- Information which might cause serious harm to the physical or mental health of the student or another individual
- Cases where the disclosure would reveal a child is at risk of abuse
- Information contained in adoption and parental order records
- Information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992
- Copies of examination scripts; and
- Providing examination marks before they are officially announced

The above are examples only of some of the exemptions under the Act.

Further exemptions may include information which identifies other individuals, information which the Academy reasonably believes is likely to cause damage or distress, or information which is subject to legal

professional privilege. The Academy will also treat as confidential any reference given by the Academy for the purpose of education, training or employment, or prospective education, training or employment.

The Academy acknowledges that an individual may have the right to access a reference relating to them received by the Academy. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

For further information on exemptions individuals may contact the DPO.

2.11 Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment will be carried out for any new policy or process which involves the processing of personal data.

3 RESPONSIBILITIES AND COMPLIANCE

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action. Data breaches carry heavy fines from the ICO, therefore it is essential that the Trust, each organisation and every member of staff are aware of their responsibilities.

3.1 Audit and Risk Committee

The Audit and Risk committee will review and approve this policy on an annual basis and recommend it to the Trust Board for ratification. Data breaches are reported annually to the Audit and Risk committee in order for them to review the effectiveness of this policy. The committee will make the appropriate resources available to support the work of the Data Protection Officer, including any necessary training.

3.2 The Senior Leadership Team

The Senior Leaders in Academies will support the work of the Data Protection Officer in implementing this policy in their institutions and ensuring the necessary processes and procedures are in place to comply with legislation. A senior member of staff in each Academy will be nominated as the named person for Data protection in their organisation.

New staff induction programmes and staff training programmes will include annual updates to Data Protection. Departments will maintain appropriate records relating to the processing of data.

3.3 Data Protection Officer

The Trust has appointed Corinne Walker as Data Protection Officer (DPO), who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. They will report to the Senior Leader stated above. Their responsibilities include:

- Inform and advise the Trust and its employees about their obligations to comply with GDPR and other data protection laws;
- To monitor compliance, train staff and conduct internal audits and Privacy Impact Assessments;
- To be the first point of contact regarding data protection issues;
- To deal with any data breaches and report a breach to the ICO if necessary.

The DPO will log Subject Access Requests, requests for data rectification or erasure and objections. The log will include details of the request and action taken.
The DPO will ensure that Data Protection Policies and Information are made available via the Trust's website.

3.4 Data Protection Committee

The Data Protection Committee will meet at least once a year and include a Data Protection Senior Leader, the Data Protection Officer, nominated data protection lead from each institution and relevant support staff from each organisation, including Trust HR Manager, Trust Head of IT, Academy Office Managers, OSFC Head of Student Services, Trust Head of Finance, as appropriate.

The role of the committee is to work with the DPO to ensure compliance at all levels, including reviewing data audits, privacy impact assessments and subject access request logs, plus determining training plans and a communication strategy relating to data protection. The Data Protection Committee will report to the Audit and Risk Committee annually.

3.5 Staff Responsibilities

Staff have access to a wide range of personal data about students, their parents and possibly employees, Governors and other third parties. All staff are required to read and understand their legal responsibilities under this policy and GDPR and attend compulsory training as required. Any data security breaches should be referred to the DPO. The Trust has Data Storage and Transfer guidance which all staff should follow.

Staff have responsibilities under the Act to ensure that data **(including computerised and manual records and <u>images</u>**) is obtained and processed fairly and lawfully in the course of your duties, whether on or off site. Staff should not collect, process, publish or disclose data in any way not described in the appropriate Privacy Statements. They should notify the DPO if they require to collect and process any additional data, this includes introducing new software into their practice. Failure to follow this policy could result in disciplinary action.

Staff need to ensure the security of data, therefore they should:

- follow the Trust Data Storage and Transfer guidance;
- before sharing data (internally or externally), check if that data can be shared with the other party;
- only store data on the Academy network which is secure and password protected;
- if personal data is accessed or stored on a home PC or personal device it must be encrypted;
- follow the Academy Remote Working Policy;
- keep IT passwords confidential and do not leave PCs in shared areas logged on when not in use; use strong passwords – at least 8 characters of mixed-case and symbols – or pick three unrelated words and do not use the same password for multiple systems;
- do not use removable/external storage devices such as USB pen drives
- double-check email addresses before pressing “send” to be sure you’re sharing personal data with intended recipients only;
- encrypt files containing personal data if they are being emailed to an external email address;
- before forwarding emails, check contents and attachments first;
- do not copy, download or forward material that is libellous or otherwise unlawful.
- Always use professional language. Do not put anything in an email message that you would not want to be read by everybody.
- make sure any websites that you are entering secure data are genuine and encrypted (check for the padlock icon next to the address bar);
- lock PC screens when away from their desk;
- keep student and employee manual records in a secure place, e.g. locked office or filing cabinets;
- do not open software storing personal info when your PC is linked to an electronic whiteboard;
- do not leave student and staff personal data where unauthorised people may see it;
- dispose of data carefully, in particular sensitive manual records should be shredded or recycled using red confidential waste bins when no longer required.
- ensure that any personal devices (phones, iPads, etc) that have access to the Academy network or email account have adequate security in terms of encryption or password/passcode protection and that Multi Factor Authentication (MFA) is installed. The device must automatically lock if inactive for

a period of time. It is your responsibility to ensure the security of data or access to the college network on your device,

Information should not be held beyond the life of its purpose; staff only have the right of access to data during their employment at the Trust. On leaving the Trust they should return or dispose of any student/staff files (either manual or computerised) and should delete data held on personal devices.

Staff should be aware that individuals can request access to all information held about them, therefore staff should ensure that records based on opinion are based on fact and worded appropriately. Emails, Teams and other messaging services must be considered open documents/ communications and **disclosable** to a wide audience

Staff should make staff/students aware if they are taking photographs of them to be used for Academy publicity or posted on social media.

3.6 External Data Processors/Third Parties

The Academy will have Processing Agreements in place for third parties contracted to process data. There will be a central record of all Processing Agreements in the Academy.

3.7 Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Academy takes any data breach seriously and will, through its policy and practice endeavour to minimise the risk of a breach. However, in the rare circumstances surrounding a data breach the Academy must inform the DPO immediately.

The GDPR states that breaches should be referred to the Information Commissioner's Office (ICO) within 72 hours of disclosure of a breach where it is likely to result in a risk to the rights and freedoms of individuals. The individual concerned must be notified where the breach is likely to result in a high risk to the rights and freedoms of individuals.

The DPO will consider the following factors before referring to the ICO :

Scale →	Content	→	Recovery	→	Assessment of Risk
How many students/staff/ other data is involved? What is the nature of the content? How sensitive is the	data? How identifiable is the data? What is the likelihood of the data being returned having not		been accessed or shared ? Can anything be done to limit the damage the breach may cause? What is the risk to rights and freedoms of individuals		concerned? What is the risk to the school, including reputational risk? Is there an ongoing risk of data loss?

The SLT link and Board of Trustees will be notified before the DPO refers an incident to the ICO.

4 COMPLAINTS AND APPEALS

If an individual believes that the Academy has not complied with this Policy or acted otherwise than in accordance with the Act, they should notify the DPO in the first instance and/or utilise the Trust Complaints Procedure if appropriate. The Complaints Procedure can be found on the Trust website.

Individuals have the right to file complaints about the processing of their personal data with the relevant

data protection authorities if they feel the Academy has not complied with their request. In case of a breach of the applicable legislation on processing of (their) personal data, individuals have the right to claim damages that such a breach may have caused them.

5 APPENDICES

Appendix 1 - Hathershaw College's Protection of Biometric Information for Children in Schools and Colleges Policy

1. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- Protection of Freedoms Act 2012
- Data Protection Act (GDPR) 2018

This policy also has regard to the following guidance:

- 'Protection of biometric information of children in schools and colleges' DfE 2018 (Updated July '22)

This policy will be implemented in conjunction with the following other policies/procedures:

- Pinnacle Learning Trust (PLT) Data Protection Policy (GDPR) 2023
- PLT Student Privacy Notice 2023 (See Appendix 1)
- General Data Protection Regulations (GDPR) – Information for Parents & Carers

2. Definitions For the purpose of this policy:

Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Biometric data is defined as personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

Automated biometric recognition system is a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint 12

scanner.

- Storing pupils/staff biometric information on a database.
- Using pupils/staff biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

3. Principles and accountability

- Biometric data will only be processed in line with the requirements of all appropriate legislation.
- Biometric data will only be processed where that processing is identified as necessary.

- The Hathershaw College will:
  - ➢ implement appropriate technical and organisational measures to demonstrate that biometric data is processed in line with the principles set out in the GDPR.
  - ➢ ensure the rights and freedoms of individuals are not adversely affected by the processing of any biometric data and that all appropriate rights as laid down by the GDPR are enforced.
  - ➢ provide comprehensive, clear and transparent privacy notices detailing the use of biometric data.
  - ➢ implement measures that meet the principles of data protection, continuously creating and improving security features.
  - ➢ produce Data Protection Impact Assessments in certain situations (See section 5 / Appendix 2)
- Any processing of biometric data will be referred to the Data Protection Officer for assessment to ensure the school fully complies with its data protection responsibilities.

4. Data protection officer (DPO)

The PLT has appointed a DPO in order to:

- inform and advise The Hathershaw College and its employees about their obligations to comply with the GDPR and other data protection laws in relation to the use of biometric data.
- monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members in relation to the processing of biometric data.

The role of DPO will be carried out by Corinne Walker.

The school will make freely available the contact details for their appointed DPO:

Corinne Walker – Trust Data Protection Officer
Oldham Sixth Form College – Union Street West, Oldham, OL8 1XU
Telephone: +44 (0) 161 287 8000 extension: 2314
Corinne Walker dataprotection@pinnaclelearningtrust.org.uk

5. Privacy by design and Data Protection Impact Assessments (DPIA's)

The school will act in accordance with the GDPR by adopting a 'privacy by design' approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into biometric processing.

DPIAs will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out:

- DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.
- A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- A DPIA may be used for more than one project, where necessary and where the aims and conditions of the project are the same.

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing where an identified risk cannot be mitigated, the school will consult the Information Commissioners Officer (ICO) to seek its opinion as to whether the processing operation complies with the GDPR

6. Consent for the use of Biometric Data

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

Where the school uses pupil and/or staff biometric data as part of an automated biometric recognition system (e.g. The Hathershaw College uses pupils' fingerprints so that they can pay for/receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

- Both parents/carers or agencies with identified parental responsibility will be informed of the plan to process biometric data.
- Written consent will be sought from at least one parent/carer of the pupil before the school collects or uses a pupil's biometric data. (See Appendix 3)
- The name and contact details of the pupil's parents/carers will be taken from the school's admission register which the school will ensure is up to date.
- Where the name of only one parent/carer is included on the admissions register, the Principal will ensure all reasonable steps are taken to ascertain the details of the other parent/carer.

The school does not need to notify a particular parent or seek their consent if it is satisfied that:

- The parent cannot be found, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts. - It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

Where neither parent of a pupil can be notified for any of the reasons set out previously, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.

Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

Details about the type of biometric information to be taken

- How the data will be used
- The parent's and the pupil's right to refuse or withdraw their consent
- The school duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

The Hathershaw College will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No parent or carer has consented in writing to the processing
- A parent has objected in writing to such processing, even if another parent has given written consent

Parents and pupils can object to participation in the school biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the school will ensure that the pupil's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent(s).

Where staff members or other adults use the school`s biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the Trust`s biometric system(s).

7. Alternative Arrangements

Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

Where an individual objects to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. at The Hathershaw College where our biometric system uses a pupil's fingerprint to pay for school meals, the pupil will be able to instead give their name the transaction instead (photographic ID to be used in this case).

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the pupil's parents/carers, where relevant).

8. Data retention

Data will not be kept for longer than is necessary in line with the schools Record Management/Retention Policy

If an individual (or a pupil's parent, where relevant) withdraws their consent for their or their child's biometric data to be processed, it will be erased from the school's system.

When a pupil or member of staff leaves the school or ceases to use the biometric system, their biometric information will be securely erased in line with the school's Records Retention Policy.

9. Policy review

This policy is reviewed annually.

The next scheduled review date for this policy is Sept 2024

Appendix 2 - PLT Student Privacy Notice 2023

Privacy Notice (How we use student information)

Students: young people aged up to 19 who are studying for qualifications at an academy of The Pinnacle Learning Trust.

The Pinnacle Learning Trust complies with the GDPR and is registered as a "Data Controller" with the Information Commissioner's Office (Reg. No. **ZA341736**). The Data Protection Officer (DPO) for the Trust is **CORINNE WALKER**. Contact details are at the end of this document.
We ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure, is retained for no longer than is necessary, and disposed of securely, in line with The Academy's Retention Policy.

The lawful basis on which we use this information

We collect the following personal data under GDPR Article 6b (Performance of a contract), GDPR Article 6c (Legal Obligation), and 6e (Public Task) in order to meet our legal obligations with the ESFA and DfE. This collection is also necessary in order for us to carry out our public task to provide education and training. The Education (Information about Individual Pupils) (England) Regulations 2013 - Regulation 5 'Provision of information by non-maintained special schools and Academies to the Secretary of State' states 'Within fourteen days of receiving a request from the Secretary of State, the proprietor of a non-maintained special school or an Academy (shall provide to the Secretary of State such of the information referred to in Schedule 1 and (where the request stipulates) in respect of such categories of pupils, or former pupils, as is so requested.' The Education Act 1996 - Section 537A – states that we provide individual pupil information as the relevant body such as the Department for Education.
Children's Act 1989 – Section 83 – places a duty on the Secretary of State or others to conduct research.

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address, parent/guardian)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Medical conditions
- Special Educational Needs and Disability
- Behaviour and exclusions
- Education/school history
- Siblings information

Why we collect and use this information

We use the student data:

- to support student learning
- to support student welfare
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard students
- the prevention and detection of crime

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

What if I do not provide personal data?

Failure to provide data required to meet legal obligations will result in us not being able to enrol you as a student. Failure to provide other information (except that requiring consent), for example learning difficulty or disability information, may result in the college being unable to provide the standard of service we would wish to provide.

Who do we share student information with?

We routinely share student information with:

- Educational establishments that the student attends after leaving us
- our local authority
- the Department for Education (DfE) / Education and Skills Funding Agency (ESFA)
- NHS/school nurse
- Third party professional services i.e. Social Services, Social Care Teams
- Agencies that provide services on our behalf
- Third-party organisations, as allowed by law
- Employers (references, work experience)
- Parents of students

Why do we share student information?

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) / Education and Skills Funding Agency (EFSA) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013

How do we store and secure data?

Data is stored in a range of different places, including the student information management systems, on paper in stored secure places, or on electronic documents within a secure network.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

CCTV

All Trust academies use CCTV systems to ensure the safety and security of all students, staff and visitors. All footage is stored for no longer than six weeks and is automatically overwritten, unless it is to be used in evidence for a criminal case.

CCTV cameras are sited to ensure that only public or common areas within the Trust sites are recorded. The

cameras are positioned so that no members of the public are inadvertently recorded.

In addition, Oldham Sixth Form College operates a Body-Worn Camera system that can record audio and visual footage. These cameras are limited to use by the security team. All policies are available on the Trust website.

Monitoring

Students should be aware that the Trust monitors activity on its ICT facilities in order to provide a safe environment for children and young people. Inappropriate activity (even personal communication) will be reported to the DSL and/or Principal, which may result in disciplinary action.

Photographs

The Academies within the Trust may take photographs, videos or webcam recordings of students for official use, monitoring and for educational purposes. You will be made aware that this is happening and the context in which the photograph will be used.

Photographs may also be taken of those attending events which may appear in the newspaper or marketing materials. You will be made aware that this is happening and the context in which the photograph will be used.

Do the Academies use automated decision-making?

Oldham Sixth Form College uses an automated process to send absence notifications.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools, or for students over 16, the Education and Skills Funding Agency privacy statement https://www.gov.uk/government/publications/privacy-notice-for-key-stage-5-and-adult-education

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth be passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of 18

youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers
- For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law to provide information about our school students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our school students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of: ● who is requesting the data

- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received To contact DfE: https://www.gov.uk/contact-dfe

Learning Records Service (LRS)

The Learning Records Service is operated by the Skills Funding Agency. The Learning Records Service collects data relating to learners registering for relevant post-14 qualifications, for example GCSEs and A-Levels. The Learning Records Service stores learner participation and achievement data collected directly from awarding organisations. This information is known as the 'Personal Learning Record' (PLR). Permitted organisations will have access to a student's PLR in order to access their achievements, awards and to enable advice and guidance to be provided. Students, as the learner, will be able to get a copy of their PLR. In addition

to the Personal Learning Record, the Learning Records Service provides a Unique Learner Number (ULN) to individual learners.

For more information about how your information is processed and shared refer to the Extended Privacy Notice available on Gov.UK.

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Data Protection Officer (details are below)

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, please raise your concern with us in the first instance. Our DPO (Data Protection Officer) is **CORINNE WALKER** and details of how to contact her are at the end of this document.
Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Withdrawal of Consent

The lawful basis upon which the Trust processes personal data is that it is necessary in order to comply with the Trusts legal obligations and to enable it to perform tasks carried out in the public interest. Where the Trust processes personal data **solely** on the basis that you have consented to the processing, you will have the right to withdraw that consent.

Further Information

If you would like to discuss anything in this privacy notice, please contact:
Corinne Walker, Data Protection Officer, The Pinnacle Learning Trust
C/o Oldham Sixth Form College, Union Street West, Oldham, OL8 1XU

Tel: 0161 287 8000 ext 2314
Email: dataprotection@pinnaclelearningtrust.org.uk

Changes to this privacy notice

We may change this privacy notice and we encourage you to check this privacy notice from time to time

ppendix 3 - Data protection Impact Assessments (DPIA)

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	

Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**

		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/ date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion

Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by: Comments:		If overruled, you must explain your reasons
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 4 – Template notification and consent form

General Data Protection Regulations (GDPR) – Information for Parents & Carers Name

of student Year group: _____

I acknowledge that the College needs to hold certain information about my child in order to operate and provide their education.

Section 1 – Information we have to collect and process

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address, parent/guardian) ● Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Biometric data in the form of your child's finger print to enable the purchase of food ● Assessment information
- Medical conditions
- Special Educational Needs and Disability
- Behaviour and exclusion
- Education/school history
- Sibling information

We do not need approval from you to hold and process this information as the GDPR has categorised it as being necessary for us to operate efficiently and safely. We are, however, required to keep this information secure, use it for the intended purpose and delete it when it is no longer required.

Section 2 – Right to access

Under the GDPR, it is your right to request access to the information that we hold on you or your child. If you wish to exercise this right, please inform the College Principal in writing. There is no charge for this service.

Section 3 – Right to have information removed

If you believe that any of the information we hold on your child is incorrect, please inform the College in writing. If we agree that the information is inaccurate, we will either change this or remove it from your child's school record.

Section 4 – Additional information

We would like to be able to hold photographs of your child to celebrate their success and for use in marketing materials. I am sure you will agree that it is always good to see a picture or video of your child engaged in learning and enjoying school.

I agree to images of my child being taken for use in marketing or publicity materials

I do not want images of my child to be used in marketing or publicity materials

Signed (parent/carer).....Date……