Frontier Learning Trust

Data Protection Policy

Approved by	Audit & Compliance Committee
Approval Date	October 2025
Review Date	September 2026

Introduction

Frontier Learning Trust needs to keep certain information about students, staff, governors and other stakeholders to allow its schools and colleges to deliver teaching and learning, monitor student progress, performance, achievements, and ensure the health and safety of staff and students. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully.

The Trust operates in accordance with the *UK General Data Protection Regulation (UK GDPR)*, the *Data Protection Act 2018*, and the Department for Education's guidance *Data protection in schools: record keeping and management*.

The Trust will comply with the following data protection principles and will ensure that personal information is:

- Processed in a lawful, fair and transparent manner;
- Collected for a specified and legitimate purpose – and not processed in a manner which is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- Processed in a manner that ensures appropriate security of the personal data.

Frontier Learning Trust staff and others who process or use any personal information must ensure that they follow these principles at all times.

Notification of Data Held and Processed

All staff, students, governors and other users are entitled to understand what personal information the Trust holds about them and how it is used. For example:

- what information the Trust holds and processes about them and why;
- how to gain access to it;
- how to keep it up to date;
- what the Trust is doing to comply with its obligations under UK GDPR.

The Trust will ensure that staff data is updated as and when necessary. Students' data are updated annually through the enrolment process and as necessary due to individual circumstances.

Responsibilities of Staff

All staff are responsible for maintaining their personal data held by the Trust.

All staff are responsible for checking that any information that they provide to the Trust in connection with their employment is accurate and up to date. Staff must also inform the Trust of any errors or changes e.g., changes of address or contact numbers. The Trust cannot be held responsible for any errors unless the staff member has informed the Trust of them.

If and when, as part of their responsibilities, staff collect information about other people, (e.g., about students' work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the Trust's procedures and guidance.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.

- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party. Personal information should be:

- kept on the Trust network including OneDrives, and not stored on hard drives of PCs, laptops or other devices including memory sticks, or
- kept in a locked filing cabinet, or
- in a locked drawer, or
- in a private office, or
- if it is electronic, be password-protected.

Computers where personal data can be accessed must be logged off or locked (password enabled) when the user is not in attendance.

Staff should note that Data Protection compliance is ultimately the responsibility of all staff. Individuals can be held legally responsible if they disclose personal information to any unauthorised third party. Breaches of data protection rules are considered to be a disciplinary matter, and may be considered gross misconduct in some cases.

In the event of an actual or a suspected data breach, staff should follow the data breach procedure.

Data Sharing

The Trust only shares personal data with organisations who have implemented data protection policies in line with UK GDPR guidance. The Trust outlines its processes for data sharing in its privacy notes , which includes the sharing of data for child protection purposes. These Privacy Notices are uploaded to the Trust websites and reviewed when necessary, a minimum of annually.

Where the Trust uses proprietary software subscriptions to process personal data on its behalf, it requires them to do so on the basis of written instructions, be under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data Protection Impact Assessments (DPIAs)

When the Trust is considering the introduction of any new system, service or process that involves the processing of personal data, a Data Protection Impact Assessment (DPIA) must be completed in consultation with the DPO at the procurement or planning stage.

DPIAs help to identify and mitigate privacy risks before implementation and must be approved by the DPO prior to any processing beginning.

Examples include, but are not limited to, the adoption of new software platforms, cloud-based services, biometric systems, or the introduction of technologies that involve profiling or automated decision-making.

The DPO maintains oversight of all DPIAs and advises on appropriate safeguards, lawful bases for processing, and record-keeping requirements in line with Article 35 of the *UK GDPR*.

Use of Artificial Intelligence (AI)

Our approach

The Trust recognises the growing use of Artificial Intelligence (AI) tools in education and administration. All use of AI systems must comply with data protection legislation and the principles set out in this policy.

The Trust's approach to AI is guided by four core values which shape how staff and students use AI responsibly and lawfully:

- Safety – We use AI tools in ways that protect ourselves and others, prioritising data protection, safeguarding, and risk awareness.
- Agency – We take ownership of our learning and work; AI supports but never replaces human thinking or responsibility.
- Rigour – We apply critical thinking to all outputs, evaluating accuracy, fairness, and completeness.
- Integrity – We are honest and transparent in our use of AI, declaring it where appropriate and upholding academic and professional standards.

These values link the Trust's digital and educational practice to its legal duties under the UK GDPR.

Using AI with personal data

AI systems must not be used to process, analyse, or store personal data unless a lawful basis has been identified and a Data Protection Impact Assessment (DPIA) has been completed and approved by the Data Protection Officer (DPO).

Uploading or entering identifiable data such as names, student work, images, email addresses, or any information that can directly or indirectly identify a person into public or unapproved AI tools is considered unauthorised data processing and may constitute a data breach under the UK GDPR.

Staff must seek approval from the Head of Digital Development and the DPO before using any AI system that handles personal or sensitive data.

Intellectual property and confidentiality

Student and staff work remain the intellectual property of their respective creators and/or the Trust, as outlined in the Intellectual Property Policy.

Uploading or inputting student work, teaching materials, or any other original content into an external AI system without the explicit consent of the creator and the Head of Digital Development may breach both data protection and intellectual property law.

Staff should only use AI systems approved by the Trust and must ensure that ownership and confidentiality of materials are protected.

Approved systems and safeguards

AI systems may only be used following approval through the Trust's data protection and IT governance processes. Approved systems will have appropriate contractual safeguards, including UK GDPR-compliant data processing agreements.

The Trust provides a secure, approved AI environment within its enterprise Microsoft 365 tenancy. When staff and students are logged into their Trust accounts, data processed through integrated AI tools remains within the Trust's secure infrastructure and is subject to its filtering, monitoring, and data protection controls.

Use of personal accounts or non-approved AI tools for Trust-related work, data, or student materials is prohibited. A register of approved AI tools will be maintained and reviewed annually.

AI Training and governance

All staff are required to complete periodic training on data protection and responsible AI use. Students will receive guidance on the safe and ethical use of AI as part of their digital literacy programme.

The Data Protection Officer oversees compliance with data protection legislation. The Head of Digital Development leads governance and guidance on the safe and ethical use of AI in line with the Trust's AI Values: Safety, Agency, Rigour, and Integrity.

Student Obligations

Students must ensure that all personal data provided to the Trust is accurate and up to date. They must ensure that changes of address, etc., are reported to the Main Office or via Woodle.

If students using the network process any personal data, they must ensure that they comply with the Trust's policy and the requirements of UK GDPR.

The lawful basis on which we use this information

The Trust collects personal data under UK GDPR Article 6c (Legal Obligation), and 6e (Public Task) in order to meet its legal obligations with the ESFA. This is also necessary in order to carry out the public task to provide education and training. Details on the categories of data collected and who this is shared with can be found in the privacy notices.

In addition, the Trust processes special category data under Article 9(2)(g) of the UK GDPR (substantial public interest) and Schedule 1, Part 2 of the Data Protection Act 2018, particularly for safeguarding and equal opportunities monitoring purposes.

Retention of Data

The Trust will retain student applicant data for one year after the application process has finished so that it can effectively deal with re-applications.

Information about students will be retained for a maximum of six years after they leave so that a reference can be provided or to confirm enrolment status for other reasons. As such, references cannot be provided for students who have left more than six years ago.

Child protection and safeguarding records will be retained until the year of the subject's 25th birthday, or for a minimum of six years after closure if the case did not progress to a child protection plan. Records relating to safeguarding allegations against staff will be retained until the individual reaches normal retirement age or for ten years after the allegation, whichever is longer, in line with *Keeping Children Safe in Education 2025* and IRMS guidance.

The Trust will retain staff applicant data for six months after the application process has finished so that it can effectively deal with re-applications.

Information about staff will be retained for the duration of their employment and for six years after they leave the Trust.

The retention periods set out above form the Trust's retention schedule for personal data. These are based on the *Information and Records Management Society (IRMS)* guidance for schools and academies and will be reviewed periodically to ensure they remain appropriate and compliant with statutory requirements.

Examination Marks

Students will be entitled to information about their examination marks. In line with the retention policy, past examination information will be available for six years after students leave.

Rights to Access Information

Students, parents, staff and governors have the right to access any personal data that is kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the "Subject Access Request" form and submit it to the Trust's Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The Trust will not normally charge a fee for responding to a request. A reasonable fee may only be charged where the request is manifestly unfounded or excessive.

The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month unless there is good reason for

delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Although data protection legislation affords these rights to individuals, there are circumstances where the Trust is legally required to share personal data with third parties such as the Department for Education, local authorities, or other public bodies. In such cases, these statutory obligations may override the individual's rights of access or objection.

The Right to be Forgotten

Students, parents, staff and governors have the right to obtain the erasure of their own personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the "Subject Access Request" form and submit it to the Trust Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The Trust will not normally charge a fee for responding to a request. A reasonable fee may only be charged where the request is manifestly unfounded or excessive.

The Trust aims to comply with requests as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

Training and Awareness

The Trust ensures that all staff who handle personal data receive regular training on data protection and information security.

Induction training is provided for all new staff, and annual refresher training is mandatory for all employees. Periodic reminders, updates and good-practice guidance are shared through staff bulletins and internal communications

Training covers the key principles of UK GDPR, including type of data, data handling, breach reporting, subject access requests and when to seek advice from the Data Protection Officer.

The Data Controller and the Designated Data Controller(s)

The Trust is the Data Controller under UK GDPR, and the Board of Trustees is ultimately responsible for implementation of this policy. However, the designated Data Protection Officer will deal with day-to-day matters.

Roles and Responsibilities

The Trust, as Data Controller, is responsible for determining the purposes and means of processing personal data.

Data Processors are any third parties that process data on behalf of the Trust. The Trust ensures that all processors are subject to written contracts requiring compliance with the UK GDPR, the Data Protection Act 2018, and the Trust's own data protection standards.

The **Data Protection Officer** oversees compliance with data protection legislation, provides advice and training, monitors adherence to this policy, acts as the contact point with the Information Commissioner's Office and supports schools in responding to data subject requests and data breaches.

ICO Registration

The Trust is registered with the Information Commissioner's Office (ICO) in accordance with the requirements of the Data Protection Act 2018 and UK GDPR. The registration is reviewed annually to ensure it remains accurate. Registration number: ZA885741

Data Controller: Frontier Learning Trust

Data Protection Officer

The nominated Data Protection Officer at Frontier Learning Trust is:

Data Protection Officer - Frontier Learning Trust
Judicium Consulting Limited
c/o Woodhouse College
Woodhouse Road
London
N12 9EY

dpo@frontierlearningtrust.ac.uk

020 8445 1210

Conclusion

Compliance with UK GDPR is the responsibility of all members of the Trust. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to Trust facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Protection Officer.

Each year, the Data Protection Officer will request confirmation from all functional leads that they have reviewed and are complying with this policy. The DPO will also undertake periodic audits of data protection practices across the Trust to ensure continued compliance and identify areas for improvement.

A data protection report is presented to the Audit & Compliance Committee at each meeting, with a comprehensive annual report provided at the end of the academic year summarising key activity, training, and any data breaches or risks identified.