Frank Field
Education Trust

Visitors and Contractors Privacy Notice

Policy Information:

Date prepared	October 2026
Adopted by Board	October 2026
Implementation Date	Immediate
Frequency of Review	Annually
Review Date	October 2027

Approved by CEO:



Cath Green

Approved by Chair of Board:



David Wooff

Frank Field
Education Trust

Last updated: 7 October 2026

Version: 4

Document owner: DPO

1. About this notice

This privacy notice explains how and why Frank Field Education Trust ("the Trust", "we", "us") collects and uses personal information about visitors, individual contractors, consultants, supplier contacts and personnel working for organisations that provide goods or services. It describes the information used, where it comes from, the purposes and lawful bases, recipients, retention, international transfers and information rights. It should be read with any just-in-time notice supplied for a particular service or activity.

The Trust is the controller because it decides the purposes and means of the processing described here. This notice does not create contractual rights and does not prevent the Trust from processing information where the law requires or permits it.

2. Contact details

Frank Field Education Trust can be contacted at 164 Whitby Road, Ellesmere Port, Cheshire CH65 6EA, by telephone on 0151 318 9700 or by email at info@ffet.co.uk . The Trust's ICO registration number is ZA590527.

The Data Protection Officer is Matthew Keeffe of Keeffe and Associates Ltd. The Data Protection Officer may be contacted through info@ffet.co.uk or 0151 318 9700. The Data Protection Officer advises and monitors compliance but operational decisions remain with the Trust.

3. Data protection framework

The principal legislation is the UK General Data Protection Regulation and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. The 2025 Act amends rather than replaces the existing framework. The Trust also applies the Privacy and Electronic Communications Regulations 2003 where electronic marketing or storage and access technologies are used.

Processing must be lawful, fair and transparent; limited to specified purposes; adequate, relevant and limited to what is necessary; accurate; kept no longer than necessary; and protected by appropriate security. The Trust is responsible for demonstrating compliance.

4. Information collected and sources

Detailed categories and sources appear in Schedule 1. Information may come from the individual, employer or contracting organisation, Trust host or contract manager, tender and vetting providers, the Disclosure and Barring Service, public registers, visitor and access systems, CCTV, ICT systems and people involved in an incident or enquiry.

5. Why information is used

The Trust uses the information to:

- evaluate suppliers, tenders, competence, insurance and conflicts;
- enter into and manage contracts, orders, invoicing and payment;
- identify, admit, supervise and account for people on Trust premises;
- protect pupils, staff, visitors, premises, systems and information;
- meet safeguarding, health and safety, equality, tax, fraud-prevention and legal duties;
- provide emergency assistance and reasonable access adjustments;

- investigate incidents, complaints, loss, damage, misconduct and legal claims; and
- maintain audit, security, visitor and contract records.

6. Lawful bases and required information

The Trust uses Article 6(1)(b) where processing is necessary for a contract with an individual or pre-contract steps requested by that individual; Article 6(1)(c) for legal duties; Article 6(1)(e) for public education, safeguarding and safety functions; Article 6(1)(d) in a genuine emergency; and Article 6(1)(f) for carefully assessed interests such as supplier administration, prevention of fraud, network security and claims where these are not public tasks. Consent is used only where there is a genuine choice.

Information required for identity, safeguarding, competence, insurance, site safety, contract administration, tax or payment must be provided where applicable. Without it, the Trust may refuse or delay access, engagement or payment. Health and disability information will be limited to what is necessary to make the visit or work safe and accessible.

7. Site access, safeguarding, CCTV and networks

Visitors and contractors may be required to sign in, wear identification, remain supervised or observe access restrictions. The level of checking and supervision depends on the activity, location, contact with pupils and safeguarding risk. DBS or barred-list information is processed only where the role or activity is legally eligible and the check is necessary.

CCTV and access controls may operate for safeguarding, safety, security and prevention or investigation of crime. Use of Trust networks, devices or accounts may produce access, audit and security logs. Further information is provided by the Surveillance and CCTV Policy, ICT Acceptable Use Policy and notices displayed at relevant locations.

8. Special category and criminal offence information

Special category information includes information about health, disability, racial or ethnic origin, religious or philosophical beliefs, trade union membership, political opinions, genetic or biometric identification, sex life and sexual orientation. The Trust will identify both an Article 6 lawful basis and an Article 9 condition. Where required, it will also identify a Data Protection Act 2018 Schedule 1 condition and comply with its Appropriate Policy Document.

Criminal allegation, conviction, offence, barred-list and related information is processed only under Article 10 where authorised by domestic law, including an applicable Data Protection Act 2018 condition. A DBS check or disclosure is requested only where the role or activity is eligible and the information is necessary.

9. Data sharing and processors

The Trust does not need consent every time information is shared. Sharing takes place where there is a lawful basis and is necessary, proportionate and secure. Before a non-routine disclosure, the Trust considers the recipient, purpose, authority, accuracy, data minimisation, confidentiality and secure transfer. Safeguarding information is shared in accordance with safeguarding law and guidance.

A processor handles information only on the Trust's documented instructions under a written contract containing the terms required by data protection law. Some recipients, including the Department for Education, local authorities, police, regulators, pension schemes and health bodies, may be separate controllers for their own statutory functions.

10. International transfers

Some approved service providers may store or access information outside the United Kingdom. Before a restricted transfer, the Trust will ensure that an adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, or another

lawful transfer mechanism or exception applies. The Trust will assess the transfer and apply supplementary measures where required.

11. Security

The Trust applies role-based access, authentication, secure configuration, backup, audit, training, contractual controls and incident-management arrangements appropriate to the risk. Information received or sent in error must be reported immediately. No security measure can eliminate all risk, but the Trust is required to use measures appropriate to the likelihood and severity of harm.

12. Retention

Contract, procurement, payment, supplier, visitor, CCTV, access, safeguarding and incident information is retained under the Trust's Records Management and Retention Schedules Policy. Contract records may be held for the contract term and applicable limitation, audit or statutory period. Visitor, CCTV and access records have separate periods based on purpose and any incident or preservation hold.

Routine disposal may be suspended where information is subject to a safeguarding, audit, complaint, investigation, litigation or other preservation hold. At the end of the approved period, information is securely deleted, anonymised, transferred or preserved for archival purposes where lawful.

13. Information rights

Depending on the processing and lawful basis, individuals may have the right to be informed; obtain access and a copy; correct inaccurate information; complete incomplete information; request erasure; request restriction; object to processing; receive certain information in a portable format; and withdraw consent where consent is used. Rights are not absolute. The Trust will explain any lawful restriction or refusal and the right to complain.

A request can be made verbally or in writing. The Trust may ask for proportionate evidence of identity and authority. It will normally respond within one month, subject to lawful extensions. Information about another person may be withheld or redacted where their rights or another legal duty requires this.

14. Automated decision-making

The Trust does not routinely make decisions producing legal or similarly significant effects solely by automated means. If such processing is introduced, the Trust will identify a valid lawful basis, provide meaningful information about the logic and likely consequences, and implement safeguards including the ability to make representations, obtain human intervention and challenge the decision. Additional restrictions apply where special category information is involved.

15. Data protection complaints

A data protection complaint may be made to the Trust by email, telephone or post using the contact details in section 2. The Trust will make an accessible complaints route available, acknowledge the complaint within 30 days, take appropriate steps to investigate and respond without undue delay, keep the complainant informed and communicate the outcome.

A complaint may also be made to the Information Commissioner's Office through its website, on 0303 123 1113, or at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. The ICO would normally expect the concern to have been raised with the Trust first.

16. Changes to this notice

This notice is reviewed at least annually and whenever processing changes materially. Where a new use is not reasonably compatible with the original purpose, the Trust will identify a lawful basis and provide fresh privacy information before the new processing begins unless a lawful exception applies.

Schedule 1: Categories and sources of contractor and visitor information

Purpose	Information used and source	Lawful basis and additional condition
Contact and organisation	Name, role, organisation, work contact details, host and purpose	Individual; employer; Trust host or contract manager
Identity and access	Identity evidence, photograph, badge, vehicle, arrival, departure and access records	Individual; visitor system; access control; CCTV
Contract and financial	Tender, contract, insurance, bank, tax, invoice, payment and sole-trader information	Individual; supplier; finance systems; public registers
Competence and vetting	Qualifications, licences, references, training, DBS and safeguarding checks where lawful	Individual; employer; DBS; professional bodies; vetting provider
Health and safety	Emergency, disability, adjustment, accident, incident and risk-assessment information	Individual; employer; witnesses; emergency and health professionals
Systems and security	CCTV, device, network, account, access, audit, incident and investigation records	Trust systems; approved suppliers; CCTV and security systems

Schedule 2: Purposes and lawful bases

Purpose	Information used and source	Lawful basis and additional condition
Procurement and contracting	Tender, due diligence, contact, contract, insurance and payment data	Articles 6(1)(b), (c), (e) and, where appropriate, (f).
Visitor and site management	Identity, organisation, host, vehicle, time and access information	Articles 6(1)(c), (e) and, where appropriate, (f).
Safeguarding and suitability	Identity, role, supervision, DBS and barred-list data where lawful	Articles 6(1)(c) and (e); Article 9(2)(g); Article 10 and applicable DPA 2018 conditions.
Health, safety and accessibility	Emergency, disability, accident and adjustment information	Articles 6(1)(c), (d) and (e); Articles 9(2)(b), (g), (h) or (i), as applicable.
Security, CCTV and incidents	Images, access, devices, networks, loss, damage and incidents	Articles 6(1)(c), (e) and, where appropriate, (f).
Legal, audit and regulatory matters	Contracts, correspondence, claims, investigations and disclosures	Articles 6(1)(c), (e) and, where appropriate, (f); Articles 9(2)(f) or (g) if needed.

Schedule 3: Recipients

Information may be shared with the individual's employer or contracting organisation; Trust hosts, contract managers and finance teams; visitor-management, access-control, CCTV, ICT, payment and professional-service providers; local authorities and safeguarding partners; emergency and health services; insurers, auditors and legal advisers; regulators, courts, police and government departments where necessary and lawful. The Trust will not routinely disclose visitor or contractor information for unrelated purposes.