Frank Field
Education Trust

Third Party Requests for Information

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

Contents

1. Purpose 3
2. Scope 3
3. Legal and regulatory framework 3
4. Key principles 3
5. Roles and authority 4
6. Receiving and verifying a request 4
7. Triage 4
8. Decision and authorisation 5
9. Specific request types 5
9.1 Safeguarding and section 16LA duty 5
9.2 Police requests 5
9.3 Courts and legal proceedings 5
9.4 Health and local authority requests 5
10. Informing the individual 6
11. Preparing and sending information 6
12. Recording and retention 6
13. Refusal, challenge, and escalation 6
14. Related documents and review 6
Appendix A: Third-party request and disclosure record 8
A. Request received 8
B. Requester verification 8
C. Information and purpose 8
D. Triage and legal assessment 9
E. Decision and authorisation 9
F. Disclosure and follow-up 10

1. Purpose

This procedure explains how Frank Field Education Trust receives, verifies, assesses, authorises, records, and responds to requests from external organisations or individuals for personal or confidential information about pupils, parents, carers, staff, volunteers, or other people. It is intended to support timely safeguarding and lawful public-service information sharing while preventing unnecessary or insecure disclosure.

The procedure does not replace the Trust's processes for subject access requests, freedom of information requests, educational-record requests, routine disclosures already covered by a privacy notice or data-sharing arrangement, or disclosures to the Trust's contracted processors. A request must be routed to the correct procedure according to its substance, not merely the label used by the requester.

2. Scope

This procedure applies to all Trust employees, workers, agency staff, trustees, governors, volunteers, and contractors who receive or handle a request from a third party. Third parties may include the police, local authorities, children's social care, health bodies, safeguarding partners, courts, regulators, government departments, legal representatives, insurers, professional bodies and other schools or educational settings.

It applies to verbal, telephone, email, portal, letter, and face-to-face requests, whether routine or urgent. It covers personal data, special category data, criminal offence data, safeguarding information, confidential information, and records containing information about more than one person.

3. Legal and regulatory framework

The Trust will apply the UK General Data Protection Regulation and the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025. It will also consider the Children Act 1989; the Children Act 2004, including the information-sharing duty in section 16LA; the Children's Wellbeing and Schools Act 2026; the Education Acts and regulations applicable to school records; the Human Rights Act 1998; the common law duty of confidentiality; the Crime and Disorder Act 1998; the Police and Criminal Evidence Act 1984; the Investigatory Powers Act 2016 where relevant; court rules and orders; and any other statutory power or duty identified for the particular disclosure.

The Trust will have regard to Keeping Children Safe in Education 2026, Working Together to Safeguard Children, the Department for Education's statutory Information Sharing Duty guidance issued in September 2026, Department for Education data protection guidance for schools, and the Information Commissioner's data sharing code and related guidance.

The Children Act 2004 information-sharing duty applies from 30 September 2026. Where its statutory conditions are met, relevant information must be disclosed to an eligible recipient unless the Trust considers that disclosure would be more detrimental to the child than not disclosing it. Data protection law continues to govern how information is handled and shared.

4. Key principles

Be clear about the purpose, recipient, and legal authority before disclosure.
Do not assume that consent is always required, or that a request from an official body creates an automatic right to all information requested.
Share promptly where there is a lawful safeguarding duty or an urgent need to protect life or prevent serious harm.
Share only information that is relevant, adequate, and limited to what is necessary for the stated purpose.

Check accuracy, distinguish fact from opinion and provide necessary context.
Use a secure method, verify the recipient, and restrict onward use where appropriate.
Record the request, decision, lawful basis, information disclosed or withheld, authorisation and method of transfer.
Do not promise confidentiality that cannot be maintained but avoid informing the individual were doing so would prejudice safeguarding, crime prevention, or another lawful purpose.

5. Roles and authority

The Trust Board oversees the governance framework. The Chief Executive Officer and Chief Finance & Operating Officer are responsible for implementation. Principals ensure local compliance. The Data Protection Officer advises on lawful bases, exemptions, proportionality, security, DPIAs and complex requests but does not replace operational decision-making. The Designated Safeguarding Lead leads decisions involving child safeguarding and ensures that safeguarding records are updated appropriately.

Any member of staff may share the minimum information necessary without prior approval where delay would create an immediate risk of death or serious harm, but emergency services must be contacted and the decision escalated and documented as soon as possible. In non-emergency cases, disclosure must be authorised by the role identified in section 8 or by a senior leader with delegated authority. Staff must not disclose information merely because a requester is insistent or senior.

6. Receiving and verifying a request

The recipient must establish the requester's full name, role, organisation, official contact details, identity and authority; the person or people concerned; the precise information required; the purpose; the legal power, duty or exemption relied upon; urgency; intended recipients; and any reason the individual must not be informed. Written requests should be obtained wherever practicable.

Identity and authority must be verified independently using a known official number, published organisational contact route, secure portal, or previously verified contact. Staff must not rely solely on caller identification, an email signature, a badge shown remotely or contact details supplied within an unexpected request. A request involving a court order, warrant, statutory notice, or other compulsory instrument must be referred immediately to the CFOO and DPO and, where appropriate, legal advisers.

7. Triage

The request must be classified promptly:

Emergency: an immediate and credible risk to life or serious harm requiring urgent action.

Safeguarding or welfare: information relevant to safeguarding or promoting a child's welfare, including a request within section 16LA of the Children Act 2004.

Law enforcement or regulatory: a request for prevention or detection of crime, apprehension or prosecution of offenders, taxation, regulation, or investigation.

Compulsory disclosure: a court order, warrant, statutory notice, or other binding legal requirement.
Routine public-service sharing: a request supported by a statutory function, data-sharing agreement or established approved process.

Individual rights or public access: a subject access, educational-record, freedom of information or environmental information request requiring referral to the relevant procedure.

Other third-party request: a request requiring consent, another lawful basis, legal advice, or refusal.

8. Decision and authorisation

Safeguarding disclosures concerning a child are led by the DSL, with the Principal and DPO consulted where time and circumstances permit. Emergency disclosures may be made by the most senior available member of staff or the person handling the emergency. Police, regulator, and government requests are authorised by the Principal or CFOO following DPO advice unless an emergency or an established approved process applies. Court orders, warrants, statutory notices and requests from legal representatives or insurers must be referred to the CFOO and DPO, with legal advice obtained where necessary.

The decisionmaker must identify and record an Article 6 lawful basis. Where special category data is involved, an Article 9 condition and, where required, a Data Protection Act 2018 Schedule 1 condition and appropriate policy document must also be identified. Criminal offence data requires Article 10 authority and an applicable legal condition. Consent must not be used by default where the Trust is exercising an official function, complying with law, or safeguarding a child.

The decisionmaker must consider confidentiality and Article 8 privacy rights separately from the data protection lawful basis. The assessment must address necessity, proportionality, likely benefit, potential detriment, accuracy, the child's views where appropriate, and whether the purpose can be achieved with less information. Refusal or partial disclosure must be explained to the requester where lawful and appropriate.

9. Specific request types

9.1 Safeguarding and section 16LA duty

Information relevant to safeguarding or promoting a child's welfare must not be withheld because of a mistaken belief that data protection or lack of consent prevents sharing. From 30 September 2026, where the statutory conditions in section 16LA are satisfied, the Trust must disclose relevant information to a relevant person if it considers that disclosure may facilitate that person's safeguarding or welfare functions or services, unless disclosure would be more detrimental to the child than not disclosing it. The DSL must record the relevance, recipient, anticipated benefit, proportionality, and any detriment assessment.

9.2 Police requests

The police do not have an unrestricted right to Trust records. Unless there is an emergency or compulsory legal power, the Trust should normally require a written request on an official police data-disclosure form or equivalent communication that specifies the purpose, information sought and legal basis or applicable Data Protection Act provision. The Trust must make its own decision and may narrow, defer, or refuse the request. Material should not be handed over informally to an officer without verification and authorisation.

9.3 Courts and legal proceedings

A court order, witness summons, production order, or warrant must be checked for authenticity, scope, deadline, and restrictions. The Trust must preserve potentially relevant material and must not destroy or alter it. Only information within the legal requirement should be supplied. Voluntary requests from solicitors are not equivalent to court orders and require a separate lawful basis, authority, and confidentiality assessment.

9.4 Health and local authority requests

Requests from health professionals, school nursing services, local authorities, and children's social care must be assessed by purpose and authority. Professional status alone does not justify

unrestricted disclosure. Routine sharing should follow an approved statutory return, pathway, privacy notice, or data-sharing agreement. New, high-risk, or systematic sharing may require a DPIA or revised agreement.

10. Informing the individual

The Trust should be transparent about information sharing through appropriate privacy notices and were fair and lawful, should tell the individual about a specific disclosure. The Trust need not seek consent or give advance notice where another lawful basis applies and notification would prejudice safeguarding, crime prevention, an investigation, legal proceedings, or another lawful objective. Any decision not to inform the individual must be recorded and reviewed where appropriate.

11. Preparing and sending information

Before release, the authorised person must check that the material matches the request, is accurate enough for the purpose, separates fact from opinion, contains no unnecessary third-party information, and has been redacted or summarised where this reduces risk without defeating the purpose. A second-person check should be used for sensitive, high-volume, or complex disclosures wherever practicable.

Information must be sent through an approved secure channel. Recipients and addresses must be checked immediately before sending. Passwords or access credentials must be communicated separately. Verbal disclosure should take place only after identity verification and should be followed by a contemporaneous written record. Any error or unintended disclosure must be reported immediately under the Personal Data Breach Procedure.

12. Recording and retention

Third-party disclosures must be recorded in a dedicated Information Sharing and Third-Party Disclosure Register, not the subject access request register. The record must include the request, verification, purpose, legal authority and lawful bases, decision and reasons, detriment, or proportionality assessment where applicable, information disclosed or withheld, authoriser, recipient, date, time, transmission method and any follow-up or restriction.

A proportionate note should be placed on the relevant safeguarding, pupil or staff record where it is operationally necessary, but duplicate copies should be avoided. Records must be retained under the Trust's Records Management and Retention Schedules Policy and any litigation, safeguarding, or investigation hold. A blanket 12-month deletion rule must not be applied where a longer or shorter period is justified by the record type and purpose.

13. Refusal, challenge, and escalation

A request may be refused or limited where identity or authority is not verified; the purpose or lawful basis is unclear; the request is excessive, irrelevant or insecure; disclosure would breach another legal restriction; a statutory exemption applies; or disclosure would be more detrimental to the child under section 16LA. Doubt must be escalated to the Principal, DSL, CFOO or DPO according to the issue. Urgent safeguarding must not be delayed while non-essential advice is obtained.

Complaints about data handling must be referred under the Data Protection Policy and privacy complaints process. Requests for internal review under freedom of information legislation must follow the Freedom of Information Policy. Suspected fraud, impersonation, coercion, or unlawful access must be reported to ICT, the CFOO and, where applicable, the police or regulator.

14. Related documents and review

This procedure should be read with the Data Protection Policy, Child Protection and Safeguarding Policy, Information Sharing Agreement framework, Records Management and Retention Schedules

Policy, Freedom of Information Policy, Subject Access Request Procedure, Personal Data Breach Procedure, ICT Acceptable Use Policy, Online Safety Policy and relevant privacy notices.

Training will be provided to staff who routinely receive or authorise requests. The procedure will be reviewed annually and sooner where legislation, statutory guidance, local safeguarding arrangements, or Trust systems change.

Appendix A: Third-party request and disclosure record

Complete this record for each non-routine third-party request. In an emergency, record the decision as soon as practicable after making the necessary disclosure.

A. Request received

Date and time	
Received by and role	
Method	☐ Telephone ☐ Email ☐ Letter ☐ Portal ☐ Face to face ☐ Other
Urgency claimed	
Person concerned	
Reference number	

B. Requester verification

Requester name and role	
Organisation	
Official contact details	
Identity checked by	
Independent verification method	
Authority or instrument supplied	
Request attached or saved at	

C. Information and purpose

Information requested	
Purpose and intended use	
Legal power, duty, or exemption cited	

Who will receive or access it	
Reason individual should not be informed	
Deadline	

D. Triage and legal assessment

Request category	☐ Emergency ☐ Safeguarding ☐ Police/regulator ☐ Court/statutory notice ☐ Routine sharing ☐ Information rights ☐ Other
Article 6 lawful basis	
Article 9 condition, if applicable	
DPA Schedule 1 condition / APD	
Article 10 authority, if applicable	
Confidentiality / Article 8 assessment	
Section 16LA applies?	☐ Yes ☐ No ☐ Not applicable
Potential detriment to child	
Necessity and proportionality	
DPO / legal advice obtained	

E. Decision and authorisation

Decision	☐ Disclose fully ☐ Disclose partly ☐ Defer ☐ Refuse
Reasons	
Information to be disclosed or withheld	
Individual informed?	☐ Yes ☐ No ☐ Deferred Reasons:

Authorised by and role	
Date and time	
Second-person check	

F. Disclosure and follow-up

Recipient verified immediately before release	☐ Yes ☐ No
Date and time released	
Released by and role	
Secure method used	
Summary of information released	
Restrictions or caveats communicated	
Record locations updated	
Retention rule / review date	
Follow-up action	
Incident or breach reference, if applicable	