Frank Field
Education Trust

Data Protection Policy

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

2. About this policy 3
3. Legislation and guidance 3
4. Definitions 4
5. The data controller 5
6. Roles and responsibilities 5
7. Data protection principles 6
8. Collecting personal data 6
9. Sharing personal data 8
10. Subject access requests and other rights of individuals 8
11. Parental requests to see the educational record 11
12. Biometric recognition systems 11
13. CCTV 12
14. Photographs and videos 12
15. Data protection by design and default 13
16. Data security and storage of records 13
17. Disposal of records 14
18. Personal data breaches 14
19. Training 14
20. Monitoring arrangements 15
Annex – A - Personal data breach procedure 16
Annex B – Subject Access Request Process 21
Annex C – Consent Process 26
Annex D – Managing Subcontractors and 3rd Party's Process 27

1. Overview

Frank Field Education Trust ("the Trust") recognises that the lawful, fair and secure handling of personal data is essential to the delivery of its educational, safeguarding, employment and administrative functions. The Trust is committed to protecting the rights and freedoms of pupils, students, parents and carers, employees, applicants, governors, trustees, contractors, volunteers, visitors and other individuals whose personal data it processes.

The Trust collects, creates, receives, uses, shares, stores, retains and disposes of personal data in the course of carrying out its functions. The Trust will process that information in accordance with the data protection principles and will maintain appropriate policies, records, controls and evidence to demonstrate its compliance with data protection law.

This policy sets out the standards that apply whenever personal data is processed by or on behalf of the Trust. All staff, trustees, governors, volunteers, contractors and other authorised users must comply with this policy and with any associated procedures relevant to their role.

The Trust will provide appropriate data protection training as part of induction and refresher training. Additional role-specific training will be provided to individuals whose responsibilities include handling sensitive information, responding to information rights requests, managing data breaches, procuring systems or services, administering information systems or making decisions about the use and sharing of personal data.

This policy will be made available to all staff and other persons to whom it applies. Material amendments will be communicated through the Trust's normal governance and staff communication arrangements. This policy does not form part of an employee's contract of employment, but compliance with it is a condition of authorised access to Trust information and systems.

Questions about this policy should be referred to the Data Protection Officer. The DPO advises the Trust, monitors compliance and performs the functions required by data protection law. Responsibility and accountability for compliance remain with the Trust as controller.

2. About this policy

This policy explains how the Trust will process personal data lawfully, fairly, transparently and securely. It applies whether information is collected directly from an individual, created by the Trust, obtained from another person or organisation, observed through the use of Trust systems or generated through educational, safeguarding, employment or administrative activity.

This policy applies to personal data in any format, including information held electronically, on paper, in email and messaging systems, in photographs, audio or video recordings, on portable devices, within cloud services, in structured filing systems and in any other form from which an individual is identified or identifiable.

This policy applies to processing undertaken:

- by the Trust and its academies;
- by staff, trustees, governors, volunteers and temporary workers acting on the Trust's behalf;
- by processors providing services to the Trust;
- on Trust premises or elsewhere;
- using Trust equipment or authorised personal equipment; and
- through systems hosted within or outside the United Kingdom.

Specific processing activities may also be governed by privacy notices, retention schedules, data-sharing agreements, processor contracts, information-security standards and operational procedures.

3. Legislation and guidance

This policy meets the requirements of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. It is informed by relevant guidance issued by the Information Commissioner's Office and the Department for Education.

The policy also reflects the requirements of the Protection of Freedoms Act 2012 in relation to the processing of children's biometric information and takes account of applicable ICO guidance concerning surveillance systems and personal data.

In addition, this policy has regard to the Trust's obligations under relevant education and safeguarding legislation, including the Education Act 1996, Education Act 2002, Academies Act 2010, Education (Information About Individual Pupils) (England) Regulations 2013, Children Act 1989, Children Act 2004, Equality Act 2010 and Safeguarding Vulnerable Groups Act 2006, together with the statutory guidance Keeping Children Safe in Education and other applicable safeguarding guidance.

The Education (Pupil Information) (England) Regulations 2005 will be applied where they govern the particular Trust's or processing activity. The specific parental right of access under regulation 5 applies to maintained Trust'ss and certain special Trust'ss and will not be represented as a general statutory right applying to every academy.

This policy should be read alongside the Trust's Funding Agreement, Articles of Association, privacy notices, Records Management and Retention Schedules Policy, CCTV Policy, ICT Acceptable Use Policy, information-security arrangements and associated safeguarding and information-governance procedures.

4. Definitions

TERM	DEFINITION
Personal data	means any information relating to an identified or identifiable living individual. An individual may be identifiable directly or indirectly, including by reference to a name, identification number, location data, online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership; genetic data; biometric data used for uniquely identifying an individual; data concerning health; or data concerning a person's sex life or sexual orientation.
Criminal offence data	Means personal data relating to criminal convictions and offences, allegations, investigations, proceedings, outcomes, related security measures, Disclosure and Barring Service (DBS) information and other criminal offence data processed in accordance with Article 10 UK GDPR and the Data Protection Act 2018. Criminal offence data is distinct from special category personal data and may only be processed where the Trust has identified both a lawful basis under Article 6 UK GDPR and a relevant condition under the Data Protection Act 2018.
Processing	means any operation or set of operations performed on personal data, whether or not by automated means. It includes collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, using, sharing, disclosing, restricting, erasing and destroying personal data.
Data subject	means the identified or identifiable living individual to whom personal data relates.
Data controller	means the person or organisation that, alone or jointly with others, determines the purposes and means of processing personal data.
Data processor	means a person or organisation that processes personal data on behalf of, and under the documented instructions of, a controller. A member of the controller's own staff is not a processor merely because they process personal data in the course of their duties.

Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.
Consent	means a freely given, specific, informed and unambiguous indication of an individual's wishes, given by a statement or clear affirmative action. Where explicit consent is required, it must be expressly confirmed.
Pseudonymisation	means processing personal data so that it can no longer be attributed to a particular individual without the use of additional information, provided that the additional information is kept separately and protected.
Anonymised information	means information that does not relate to an identified or identifiable individual and from which identification is not reasonably possible. Properly anonymised information is not personal data.
Data protection impact assessment or DPIA	means a documented assessment used to identify and reduce data protection risks arising from processing that is likely to result in a high risk to individuals.
Restricted transfer	means a transfer of personal data to a separate organisation outside the United Kingdom to which the UK GDPR international-transfer rules apply.

5. The data controller

Frank Field Education Trust is the controller for personal data where it determines why and how that information is processed.

The Trust's academies form part of the same legal entity and are not separate controllers merely because operational decisions are delegated locally. A Principal, member of staff, trustee or governor does not become a separate controller merely by exercising delegated responsibilities on behalf of the Trust.

Another organisation may act as:

- an independent controller where it determines its own purposes and means of processing;
- a joint controller where it determines purposes and means jointly with the Trust; or
- a processor where it acts solely on the Trust's documented instructions.

The nature of the relationship will be assessed and documented before personal data is shared or processing begins.
The Trust is registered with the ICO under registration number **ZA590527** and will maintain its registration and pay the applicable data protection fee as required.

6. Roles and responsibilities

This policy applies to trustees, governors, employees, agency workers, volunteers, contractors, consultants and other persons who are authorised to process personal data on behalf of the Trust. Processor organisations are also subject to the data protection obligations contained in their contracts with the Trust. Staff who do not comply with this policy may face disciplinary action.

6.1 Trust Board

The Trust Board has overall accountability for the Trust's compliance with data protection law. It will ensure that the Trust has appropriate governance, resources, policies, reporting arrangements, security controls and assurance mechanisms.

The Board will receive appropriate information concerning significant data protection risks, serious personal data breaches, material complaints, audit findings and the DPO's monitoring activities**.**

6.2 Data Protection Officer

The Trust has appointed a Data Protection Officer in accordance with data protection law.

The DPO will:

- inform and advise the Trust and its staff about their obligations;
- monitor compliance with data protection law, this policy and associated procedures;
- advise on DPIAs and monitor their completion;
- provide advice on personal data breaches, information rights requests, data sharing, processor contracts and international transfers;
- cooperate with the ICO and act as a contact point for the regulator;
- provide appropriate reports to the Trust Board; and
- act with independence and maintain confidentiality in the performance of the role.

The Trust will involve the DPO properly and in a timely manner in matters concerning personal data and will provide the resources and access needed to perform the role.

The DPO advises and monitors. Operational responsibility for implementing advice, maintaining systems and making controller decisions remains with the Trust and the relevant authorised decision makers.

The Trust's DPO is **Matthew Keeffe or Keeffe and Associates Ltd** and is contactable via **0151 318 9700** or via email info@ffet.co.uk .

6.3 CEO

The CEO is responsible for ensuring that this policy is implemented throughout the Trust and that appropriate senior leaders are assigned responsibility for the operational management of information governance, information security, records management and incident response.

6.4 Principals and senior leaders

Principals and senior leaders are responsible for:

- implementing this policy within their areas of responsibility;
- ensuring staff understand and follow relevant procedures;
- involving the DPO before material changes to processing are introduced;
- ensuring concerns, rights requests and suspected breaches are escalated promptly;
- ensuring access to personal data is appropriate to role; and
- completing agreed actions arising from DPIAs, audits, incidents or DPO advice.

6.5 All staff

All staff and authorised users must:

- process personal data only for authorised Trust purposes and in accordance with this policy;
- access only the information required for their duties;
- keep personal data accurate where they are responsible for maintaining it;
- use only approved systems, devices, storage locations and transfer methods;
- protect passwords, authentication methods and physical records;
- complete required training;
- recognise and promptly escalate information rights requests;
- report actual or suspected personal data breaches immediately;
- consult the DPO or relevant senior lead where unsure about lawfulness, sharing, retention, security or individual rights; and
- cooperate with investigations, audits and remedial action.

Staff must not obtain, access, use, alter, disclose, retain or destroy personal data for an unauthorised purpose.

7. Data protection principles

The Trust will comply with the principles in Article 5 UK GDPR. Personal data must be:

1. Processed lawfully, fairly and transparently.
2. Collected for specified, explicit and legitimate purposes and not further processed incompatibly with those purposes.
3. Adequate, relevant and limited to what is necessary for the identified purpose.
4. Accurate and, where necessary, kept up to date. Inaccurate information must be corrected or erased without undue delay where appropriate.
5. Kept in identifiable form for no longer than necessary, subject to lawful retention for purposes such as claims, safeguarding, archiving, research or legal obligations.
6. Processed securely, using appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, destruction or damage.

The Trust is responsible for compliance with these principles and must be able to demonstrate that compliance. This is the accountability principle.

8. Collecting personal data

8.1 Lawfulness, fairness, and transparency

The Trust will identify and document at least one lawful basis under Article 6 UK GDPR before processing personal data. The applicable lawful basis will depend upon the identified purpose and will not be selected retrospectively merely to justify processing that has already occurred.:

- The data needs to be processed so that the Trust's can **fulfil a contract** with the individual, or the individual has asked the Trust's to take specific steps before entering a contract
- The data needs to be processed so that the Trust's can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the Trust's, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests**, as a public authority, the Trust will not rely upon legitimate interests where it is processing personal data in the performance of its public tasks. Where legitimate interests is relied upon for processing outside those public tasks, the Trust will identify the interest pursued, demonstrate that the processing is necessary and balance that interest against the individual's rights and freedoms.

- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent

Where special category data is processed, the Trust will identify both an Article 6 lawful basis and a condition under Article 9 UK GDPR.

Depending upon the purpose, an Article 9 condition may include:

- explicit consent;
- employment, social-security or social-protection obligations and rights;
- protection of vital interests where the person is physically or legally incapable of consenting;
- processing of information manifestly made public by the individual;
- establishment, exercise or defence of legal claims;
- substantial public interest on the basis of UK law;
- health or social care;
- public health; or
- archiving in the public interest, scientific or historical research, or statistical purposes.

Where reliance is placed on a condition requiring an additional basis under the Data Protection Act 2018, the Trust will identify the relevant Schedule 1 condition and maintain an appropriate policy document where required.

Criminal offence data

The Trust may process criminal offence data where it is necessary and lawful to do so, including for safeguarding, safer recruitment, employment management, disciplinary matters, regulatory compliance, legal claims, security and the protection of pupils, staff and visitors. Criminal offence data will only be processed where:

- the Trust has identified a lawful basis under Article 6 UK GDPR;
- the Trust has identified a condition under Schedule 1 of the Data Protection Act 2018 or is otherwise authorised to process such information;
- the processing is necessary and proportionate for the purpose identified;
- access is restricted to authorised individuals; and
- appropriate security and retention measures are in place.

Criminal offence data will not be collected, used or disclosed unless there is a clear legal basis for doing so.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, minimisation, and accuracy

The Trust will collect personal data only for specified, explicit and legitimate purposes. Individuals will be given appropriate information about those purposes in accordance with the Trust's privacy notices.

Before using personal data for a new purpose, the Trust will determine whether the new purpose is

compatible with the purpose for which the information was originally collected. Where the new purpose is not compatible, the Trust will identify a new lawful basis and provide any additional privacy information required before the new processing begins. Consent will only be sought where it is the appropriate lawful basis.

Personal data must be adequate, relevant and limited to what is reasonably necessary for the identified purpose. Staff must not collect, create, copy, retain or share personal data merely because it may be useful at some unspecified future date.

The Trust will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. Inaccurate personal data will be rectified or erased without undue delay where appropriate.

Personal data must be retained and disposed of in accordance with the Trust's Records Management and Retention Schedules Policy. Staff must not independently delete, destroy or anonymise official records unless authorised to do so under the applicable retention and disposal arrangements.

9. Sharing personal data

The Trust will share personal data only where the disclosure is lawful, necessary, proportionate and limited to the information reasonably required for the identified purpose.

Consent is not required for every disclosure. The Trust may share personal data without consent where another lawful basis applies, including where sharing is necessary:

- to perform the Trust's education or other public functions;
- to comply with a legal obligation;
- for safeguarding and child protection;
- to protect the vital interests of an individual;
- for law-enforcement or regulatory purposes where the applicable legal conditions are met;
- for the establishment, exercise or defence of legal claims;
- to respond to an emergency; or
- to enable an authorised processor to provide services on the Trust's behalf.

Where special category or criminal offence data is shared, the Trust will also identify and document the applicable additional condition under the UK GDPR and Data Protection Act 2018.

Before making a non-routine disclosure, the Trust will consider and, where appropriate, record:

- the identity and authority of the recipient;
- the purpose of the disclosure;
- the applicable Article 6 lawful basis;
- any applicable Article 9, Article 10 or Data Protection Act 2018 condition;

- whether disclosure is necessary and proportionate;
- the minimum personal data required;
- whether the recipient is a controller, joint controller or processor;
- the security of the proposed transfer; and
- whether the disclosure is covered by the relevant privacy information.

Data protection law must not be treated as a barrier to necessary and proportionate safeguarding information sharing. Staff must follow the Trust's safeguarding procedures and refer safeguarding disclosures to the Designated Safeguarding Lead or authorised deputy. The decision, reasons, recipient and information shared will be recorded where appropriate.

Where a processor handles personal data on the Trust's behalf, the Trust will:

- carry out proportionate due diligence;
- use only processors providing sufficient guarantees of appropriate technical and organisational measures;
- put in place a written contract meeting Article 28 UK GDPR;
- ensure that the processor acts only on documented instructions;
- address confidentiality, security, sub-processors, breaches, information rights, audits and deletion or return of personal data;
- review the arrangement as appropriate during the contract; and
- ensure the processing ends appropriately when the service terminates.

Where the Trust and another controller jointly determine the purposes and means of processing, their respective responsibilities will be set out in a transparent joint-controller arrangement where required.

A restricted transfer of personal data outside the United Kingdom will only take place where it is covered by applicable UK adequacy regulations, an appropriate safeguard permitted by the UK GDPR or a statutory exception. Where required, the Trust will complete and document a transfer risk assessment or data protection test and implement any necessary supplementary safeguards.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have the right, subject to the applicable statutory conditions and exemptions, to obtain confirmation as to whether the Trust processes their personal data and to receive:

- a copy of that personal data;
- the purposes of processing;
- the categories of personal data concerned;
- the recipients or categories of recipients;

- the applicable retention period or the criteria used to determine it;
- information about the rights to rectification, erasure, restriction and objection;
- information about the right to complain to the ICO;
- the source of information not obtained from the individual;
- relevant information about automated decision-making and its consequences; and
- information about safeguards applying to a relevant international transfer.

A subject access request may be made verbally or in writing. It does not have to mention the UK GDPR, use specific wording or be submitted on a Trust form.

Any member of staff receiving a request that may amount to a subject access request must forward it without delay to the Data Protection Officer and the Trust officer responsible for coordinating information rights requests.

The Trust will carry out a reasonable and proportionate search for personal data within the scope of the request. In determining what is reasonable and proportionate, the Trust will consider:

- the circumstances and scope of the request;
- the volume of information that may need to be searched;
- the accessibility of that information;
- any difficulty involved in locating or retrieving it; and
- the fundamental importance of the right of access.

A decision that a particular search would be unreasonable or disproportionate must be justified and documented. Where one part of a proposed search would be disproportionate, the Trust will continue to search other locations falling within the scope of the request.

The Trust may ask the individual for information reasonably required to identify the personal data or processing activities to which the request relates. The Trust may also request evidence reasonably necessary to verify identity where it has reasonable doubts about the requester's identity. It will not routinely require two forms of identification or request more information than is necessary.

10.2 Children and subject access requests

Personal data relating to a child belongs to the child. Whether a child is competent to exercise the right of access independently will be assessed individually.

The Trust will consider:

- the child's age, maturity and ability to understand the request and its consequences;
- the nature and sensitivity of the information;
- the child's wishes;
- the requester's authority to act;
- the child's best interests;

- any safeguarding concerns; and
- the rights and freedoms of other individuals.

No fixed age will be treated as determinative in every case.

Where a parent or representative submits a request on behalf of a competent child, the Trust will normally seek appropriate evidence that the child authorises the representative to act. Where the child is not competent to make the request independently, the Trust will consider whether the requester has authority to act and whether disclosure is in the child's best interests.

10.3 Responding to subject access requests

When responding to a subject access request, the Trust will:

- acknowledge receipt of the request as soon as reasonably practicable;
- record the request in the Trust's SAR Register;
- verify the identity of the requester, or the authority of a representative acting on their behalf, where this is reasonably necessary;
- contact the requester where clarification is required to identify the personal data or processing activities to which the request relates;
- conduct a reasonable and proportionate search for personal data falling within the scope of the request;
- assess whether any statutory exemptions or restrictions apply;
- provide the information in a secure and accessible format; and
- maintain an audit trail of the searches undertaken, decisions made and information disclosed.

Where the Trust has reasonable doubts about the identity of the requester, the statutory response period will not begin until sufficient information has been provided to verify identity. The Trust will only request identification information that is reasonable and proportionate in the circumstances and will not routinely require two forms of identification.

Where a request is submitted by a solicitor, parent, guardian, trade union representative or other third party, the Trust may request evidence of authority to act on behalf of the data subject before processing the request.

The Trust will respond without undue delay and within the statutory response period. Where a request is complex or the individual has made a number of requests, the Trust may extend the response period by up to two further months. The individual will be notified of the extension and the reasons for it within the initial response period.

Information will generally be supplied free of charge. The Trust may charge a reasonable fee or refuse to act only where the request is manifestly unfounded or excessive, or where additional copies of information already supplied are requested.

Before withholding any information, the Trust will identify the specific statutory exemption or restriction relied upon and apply it to the particular circumstances of the request. Information will not be withheld solely because it relates to a sensitive subject matter.

Where information contains personal data relating to another individual, the Trust will consider whether it is reasonable to disclose that information having regard to all relevant circumstances and may redact or otherwise protect third-party information where appropriate.

Where the Trust refuses to act on all or part of a request, it will explain:

- the reasons for its decision;
- the right to make a data protection complaint to the Trust;
- the right to complain to the Information Commissioner's Office; and
- the right to seek a judicial remedy.

11. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified based on public interest, official authority, or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their personal data with no human involvement) and be able to request human intervention
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine- readable format (in certain circumstances)
- Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the educational record

Parents, or those with parental responsibility, do not have an automatic statutory right to inspect or obtain a copy of a child's educational record under the Education (Pupil Information) (England) Regulations 2005 where the child attends an academy within the Trust.

Requests for information relating to a child will ordinarily be considered under the UK GDPR and the Data Protection Act 2018, taking account of:

- the child's right to privacy;
- the child's age, maturity and ability to understand their data protection rights;
- the authority of the parent or representative making the request;
- the child's wishes and best interests;
- safeguarding considerations; and
- the rights and freedoms of other individuals.

The Trust will consider each request on its individual circumstances and may provide information where it is lawful, fair and appropriate to do so.

There may be circumstances where information cannot be disclosed, including where disclosure:

- could cause serious harm to the physical or mental health of the child or another individual;
- would prejudice the welfare or safeguarding of a child;
- would disclose personal data relating to another individual where disclosure would not be lawful;
- is subject to a statutory exemption under data protection legislation; or
- is otherwise restricted by law.

Educational information held by the Trust may include, but is not limited to:

- attendance information;
- behaviour records;
- assessment and examination results;
- Trust's reports;
- curriculum and progress information;
- timetable information;
- disciplinary records;
- admissions information;
- personal details relating to the pupil; and
- details of previous educational establishments attended.

Nothing in this section prevents the Trust from sharing appropriate educational, pastoral, safeguarding, attendance or progress information with parents or those with parental responsibility where it is lawful and appropriate to do so.

13. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive Trust's dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The trust will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the Trust's's biometric system(s). We

will provide alternative means of accessing the relevant services for those pupils. For example, students can pay for lunch using a card system.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the Trust's's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the trust will delete any relevant data already captured.

14. CCTV

We use CCTV in various locations around Trust's sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the individual CCTV systems should be directed to the Trust's office of the Trust's your child attends alternatively you can Data Protection Officer on 0151 318 9700 or via email: info@ffet.co.uk .

For further information please refer to the appropriate trust's CCTV policy.

15. Photographs and videos

As part of our trust activities, we may take photographs and record images of individuals within our trust.

We will obtain written consent from parents/carers, students or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing, and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at Trust's events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (students or pupils where appropriate) have agreed to this.

Where the trust takes photographs and videos, uses may include:

- Within Trust's on notice boards and in Trust's magazines, brochures, newsletters, etc.
- Outside of Trust's by external agencies such as the Trust's newspapers, campaigns
- Online on our Trust's and trust website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the

photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the Trust's's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we complete a UK restricted transfer, where different data protection laws will apply
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our Trust's and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

17. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out
- Passwords and authentication methods used to access Trust systems must comply with the Trust's ICT and Information Security requirements. Where available, multi-factor authentication will be implemented to further protect access to systems containing personal data.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Personal data should only be stored or accessed using personal devices where authorised by the Trust and where appropriate security measures are in place, including device security, access controls and encryption where required.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

Access to personal data will be restricted to those individuals who require it to perform their role. The Trust will periodically review access permissions and ensure access is removed or amended when responsibilities change.

18. Retention and Disposal of records

Personal data will be retained in accordance with the Trust's Records Management and Retention Schedules Policy and any other applicable legal or regulatory requirements.

Personal data must not be destroyed where it is relevant to:

- a safeguarding matter;
- a subject access request;
- an information rights request;
- a complaint or grievance;
- disciplinary proceedings;
- a legal claim or potential legal claim;
- a regulatory investigation; or
- any other matter requiring preservation of records.

Once the applicable retention period has expired, personal data will be securely destroyed, permanently deleted or anonymised as appropriate.

Where a third party is used to dispose of records or equipment, the Trust will ensure that suitable contractual and security arrangements are in place and may require evidence of secure destruction.

19. Personal data breaches

The Trust will take all reasonable steps to prevent personal data breaches. However, a personal data breach may occur through accidental or deliberate action and may include the loss, destruction, alteration, unauthorised disclosure of, or access to, personal data.

Any member of staff who becomes aware of an actual or suspected personal data breach must report it

immediately in accordance with Annex A of this policy.

The Trust will investigate all reported breaches, take appropriate containment measures and assess the risks to affected individuals.

Where required by law, the Trust will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of a reportable personal data breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust will also notify affected individuals without undue delay unless an exemption applies.

20. Complaints Process for Data Subjects

Individuals who have concerns about how the Trust has collected, used or handled their personal data are encouraged to raise those concerns with the Trust in the first instance.

The Trust will investigate data protection complaints fairly and promptly and will keep appropriate records of complaints received, investigations undertaken and actions taken.

Raising a complaint with the Trust does not affect an individual's right to complain directly to the Information Commissioner's Office at any time.

21. Responsible Use of Artificial Intelligence (AI)

The Trust may use approved artificial intelligence tools and technologies to support educational, administrative and operational activities where this is lawful and appropriate.

Before personal data is processed using artificial intelligence technologies, the Trust will consider data protection, safeguarding, security and equality implications and undertake a Data Protection Impact Assessment where required.

Staff must not input confidential, safeguarding, employment or other personal data into unapproved artificial intelligence systems.

Any information or output generated using artificial intelligence must be reviewed by an appropriate member of staff before it is relied upon or used for decision-making.

22.Training

All staff, trustees and governors will receive appropriate data protection training as part of their induction.

Refresher training and updates will be provided periodically and whenever significant changes to legislation, guidance, technology or Trust procedures occur.

Additional role-specific training may be provided to individuals whose responsibilities involve significant processing of personal data, safeguarding information, information rights requests or information security matters.

The Trust will maintain appropriate records of training completed.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust’s’s processes make it necessary.

23. Monitoring arrangements

Compliance with this policy will be monitored by the Data Protection Officer, senior leaders and other authorised personnel through audits, reviews, breach monitoring, information rights trends, complaints and compliance activities.

Findings may be reported to senior leaders, the Trust Board and other governance bodies as appropriate.

This policy will be reviewed annually or earlier where there are significant changes in legislation, regulatory guidance, organisational arrangements or processing activities.

24. Links with other policies

This policy should be read alongside:

- Records Management and Retention Schedules Policy;
- Freedom of Information Policy and Publication Scheme;
- ICT Acceptable Use Policy;
- CCTV Policy;
- Information Security procedures;
- Safeguarding and Child Protection Policy;
- Online Safety Policy;
- Whistleblowing Policy; and
- Staff Disciplinary Policy and Procedure.

Annex – A - Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On becoming aware of an actual or suspected personal data breach, staff, contractors and data processors must immediately notify the DPO, CEO, CFOO or other nominated reporting contact in accordance with this procedure.
- The DPO, supported by relevant Trust staff, will assess the incident, establish the facts, identify the information involved and determine whether a personal data breach has occurred.
- Appropriate steps will be taken immediately to contain the incident and minimise any risk to affected individuals.
- The Trust will assess:
    - the nature of the personal data involved;
    - the number of individuals affected;
    - whether special category or criminal offence data is involved;
    - whether the information has been accessed, disclosed, altered, lost or destroyed;
    - the likelihood of harm occurring; and
    - the severity of any potential consequences.
- The DPO will advise whether notification to the Information Commissioner's Office and affected individuals is required.
- All breaches will be documented on the Trust's breach register together with the outcome of the investigation and any corrective actions taken.
- Following closure of the incident, the Trust will review lessons learned and implement any necessary procedural, technical or organisational improvements.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Trust will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Trust will also notify affected individuals without undue delay unless a lawful exemption applies..

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the Trust's computer system.
- The DPO and CFOO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT representative to recall it*

  In any cases where the recall is unsuccessful, the Sender will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- *The Trust will take reasonable and proportionate steps to obtain confirmation that information has been securely deleted and has not been further used or disclosed. The actions taken will depend on the circumstances of the breach and the level of risk presented.*
- *The ICT representative or DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

***Other types of breach that you might want to consider could include**:*

- *Details of pupil premium interventions for named children being published on the Trust website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A Trust laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The Trust's parent payment provider being hacked and parents' financial details stolen*

Consequences of Failing to Report a Breach

Failure to report an actual or suspected personal data breach promptly may increase the risk of harm to individuals and may prevent the Trust from meeting its legal obligations.

All staff are therefore required to report actual or suspected breaches immediately through the procedures contained within this policy.

Failure to comply with Trust procedures may result in disciplinary action where appropriate.

So, it's important that staff follow the breach-reporting process in place within this policy and to ensure we recognise, detect via our IT Team and can notify a breach, on time; and to provide the necessary details. We shall use the ICO breach reporting form for this purpose as follows https://ico.org.uk/media/for-organisations/documents/2614197/personal-data-breach-report-form-web-20190124.doc .

It is imperative that, where staff feel a breach has occurred, they report this to the DPO, CEO or the Chief Finance & Operating Officer via **Appendix 1** at the earliest opportunity.

Appendix 1 – Staff Internal Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the DPO immediately. The breach will be recorded on the Trusts' Breach Register and the Trustees' and DPO will be informed so that an investigation can be carried out		
	Report by:	
	Date	
1	**Nature of breach e.g. theft/disclosed in error/technical problem**	
2	**Description of how breach occurred:**	
3	**When was the breach reported and how did you become aware?**	
4	**Full description of all personal data involved**	
5	**Number of individuals affected?** **Have all individuals affected been informed**	
6	**What immediate remedial action was taken:**	
7	**Has the data been retrieved or deleted? If yes – date and time:**	
8	**Any Procedure changes needed to reduce risks of future data loss**	

9	**Conclusion**	

NB: Please return this form to the Chief Finance & Operating Officer, CEO or our DPO.

Annex B – Subject Access Request Process

Introduction
All personal data processed by Frank Field Education Trust is within the scope of this policy. Personal data that is asked for as a matter of routine e.g. copies of employment contracts, job descriptions or other information already received by data subjects.

Data subjects are entitled to ask:
• Whether Frank Field Education Trust is processing any personal data about that individual and, if so, to be given:
- a description of the personal data;
- the purposes for which it is being processed; and,
- details of who will be allowed to see the personal data.

• To be given a copy of the information and to be told about the sources from which Frank Field Education Trust derived the information.

Responsibilities
The CEO is responsible for the application and effective working of this policy and procedure, and for reporting to the Board of Trustees on Subject Access Requests (SARs).

The Chief Finance & Operating Officer and her team are responsible for handling all SARs, with the advice and guidance of the Data Protection Officer.

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the Chief Finance & Operating Officer.

Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Records of Subject Access Requests, searches undertaken, decisions made, disclosures issued and any exemptions applied will be retained in accordance with the Trust's Records Management and Retention Schedules Policy.

The Trust will consider requests relating to children on a case-by-case basis, taking account of the child's age, maturity, understanding, wishes, safeguarding considerations and the authority of the person making the request.

No fixed age will automatically determine whether a child is able to exercise their data protection rights independently.

Responding to subject access requests – Procedure

When responding to requests, we:

- The Trust has provided a Subject Access Request Form ('**Subject Access Request (Form)**'at **Appendix 1)** to help individuals describe the information they require. Use of the form is optional and requests will not be refused because a particular form has not been used.
- Where the Trust has reasonable doubts regarding an individual's identity, it may request sufficient information or documentary evidence to verify identity before processing the request. The Trust will only request information that is reasonable and proportionate in the circumstances.
- May contact the individual via phone to confirm the request was made
- Request the Data Subjects permission to disclose the data to a parent or guardian
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

Collection will entail either:

- Collecting the data specified by the data subject, or

- The Trust will undertake a reasonable and proportionate search of systems, records and repositories that are likely to contain information falling within the scope of the request.
- Archived material and backup systems will be considered where the information remains accessible and searching them would be reasonable and proportionate in the circumstances.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Information covered by legal professional privilege
- Negotiations with the data subject in relation to the request

- Information for crime prevention or detection
- Management forecasts
- Information used for research, historical or statistical purposes

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Supplying the data to the data subject
The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on the '**Responding to a Subject Access Request (Form)**' at **Appendix 2** that shows the data subject's name and the date on which the information is delivered.
The electronic formats used for responses to SARs are:

CSV files;
Excel files;
Word files;

All machine-readable transitions require a robust level of encryption to send the information to a data subject and or transmit that data to another controller, at the written request of the Data Subject.

Appendix 1 to Subject Access Process

Subject Access Request (Request Form)

[Insert date]

insert your Trust name and address

Re: subject access request

Dear *Trust,*

Please provide me with the information about me that I am entitled to under the UK General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the Trust	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *My personnel file* • *My child's medical records* • *My child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.
Please bear in mind that, in most cases, you must supply me with the information within 1 month and free of charge.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

[Insert Name]

Appendix 2 to Subject Access Process

Responding to a Subject Access Request (Form)

[Insert date]

Insert your Trust's name and address

Re: subject access request

Dear *insert the name of the individual who submitted the subject access request*

Please find enclosed the information that you requested under the UK General Data Protection Regulation (UK GDPR).

Your name	
Your relationship with the Trust	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Details of the information you requested/enclosed	*Insert details of the specific information requested, such as:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*
Date you requested the information	
Date we supplied the information	*This must be within one month of the above date*
Format we supplied the information	*For example, encrypted USB stick accompanying this letter*

[Ensure we send the data either manually or electronically and record a copy on the Trusts Server]

If you need any further advice relating to your subject access request, you can contact:

The CFOO on 0151 318 9700 or Matthew Keeffe – Data Protection Officer – via info@ffet.co.uk stating the Trust your enquiry is relating to.

Annex C – Consent Process

1. Scope

Where, in accordance with the UK GDPR, the consent of the data subject is required for the processing of his or her personal data, it will be within the scope of this procedure.
Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Consent will not be relied upon where an individual does not have a genuine and freely exercisable choice or where another lawful basis more appropriately reflects the processing activity being undertaken.

2. Responsibilities

The data controller, Frank Field Education Trust is responsible under the UK GDPR for obtaining consent from the data subject under advisement from the Data Protection Officer.

3. Consent procedure

3.1 Frank Field Education Trust shall be able to demonstrate that valid consent has been obtained where consent is relied upon as the lawful basis for processing.

Explicit consent will only be obtained where required by law or where the Trust has determined that explicit consent is the most appropriate basis for the processing activity. (Consent Form – Pupil, Staff Member or Trustee).

3.2 Frank Field Education Trust shall be able to demonstrate that the data subject has consented to the processing of his or her personal data for one or more specific purposes (Consent Form – Pupil, Staff Member or Trustee).

3.3 Frank Field Education Trust shall be able to demonstrate that the data subjects' consent is easily distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use the Consent Form – Pupil, Staff Member or Trustee, or email then attach the email to the form).

3.4 Frank Field Education Trust shall be able to demonstrate that the data subjects' consent is in an intelligible and easily accessible format using clear and plain language.

3.5 Frank Field Education Trust shall be able to demonstrate that the data subject has been informed of their right to withdraw consent before giving consent.

3.6 Frank Field Education Trust shall be able to demonstrate that processing of data is limited to the contract bound by the explicit consent given by the data subject.

4. Withdrawal of consent procedure

4.1 Individuals may withdraw consent at any time.

Where consent is withdrawn, the Trust will:

- record the withdrawal;
- stop any future processing that relies solely upon that consent;
- inform relevant staff and processors where appropriate;

- explain whether another lawful basis applies; and
- update records where necessary.

Withdrawal of consent does not affect processing that was lawful before consent was withdrawn.

Annex D – Managing Subcontractors and 3rd Party's Process

1. Scope

All external suppliers that process personal data on behalf of Frank Field Education Trust are within the scope of this procedure.

2. Responsibilities

2.1 The CFOO, Finance Managers and Data Protection Officer in conjunction with the Finance Department are responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this procedure.

2.2 The owners of third-party relationships are responsible for ensuring that all data processing is carried out in line with this procedure.

2.3 The IT Representative is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.

2.4 The Finance Managers are responsible for carrying out regular audits of contractor or third-party compliance. This may involve requiring the supplier to sign a non disclosure agreement where they have access to special category or high volumes of personal data to complete their contractual obligations.

3. Procedure

3.1 Frank Field Education Trust selects only suppliers that can provide technical, physical and organisational security that meet Frank Field Education Trust's requirements in terms of all the personal information they will process on Frank Field Education Trust's behalf.

Prior to appointment, the Trust will carry out proportionate due diligence which may include consideration of:

f

- security arrangements;
- certifications;
- cyber security controls;
- breach history;
- international processing locations;
- sub-processors;
- business continuity arrangements;
- deletion and exit processes; and
- the supplier's ability to comply with UK data protection legislation.

3.2 Where a supplier or processor stores, accesses or processes personal data outside the United Kingdom, the Trust will assess whether a restricted transfer occurs and ensure that an appropriate transfer mechanism and safeguard is in place before processing begins.

3.3 An information security risk assessment, is carried out before a supplier is engaged (See **Appendix 1**) and, if the Finance Managers considers it necessary because of the nature of the personal information to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements against the requirements of Cyber Essentials may be conducted before entering into the contract.

3.4 Frank Field Education Trust requires a written agreement (See **Appendix 2**) to provide the service

as specified and requires the supplier to provide appropriate security for the personal information it will process.

3.5 All data processing contracts allow Frank Field Education Trust to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal information.

3.6 All data processing contracts forbid suppliers from using further subcontractors without Frank Field Education Trust's written authorization for the processing of personal information.

3.7 Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the supplier) if they specify that, when the contract is terminated, related personal information will either be destroyed or returned to Frank Field Education Trust.

Appendix 1 to Managing Sub-Contractors and 3rd Parties Process

DRAFT LETTER AND INFORMATION SECURITY QUESTIONNAIRE FOR SUB CONTRACTORS AND 3RD PARTIES

Date:

[Insert Supplier Name and Address}

Dear Sir/Madam,

UK GDPR Compliance

As an Trust we are continually working towards ensuring compliance with the UK GDPR and the Data Protection Act 2018.

As a sub-contractor or 3rd party supplier you need to confirm that you have undertaken the necessary review of your processes and procedures to comply with the changes. To continue with our commercial relationship, we need confirmation of this and agreement that the current contract or arrangements will be agreed and amended to reflect this.

Please complete the series of questions below and explain how you will comply.

We require the form to be completed, signed and returned to us. We reserve the right to request any additional information from you about your processes and procedures that will enable us secure compliance with the UK GDPR requirements.

As a public authority we have an obligation to be compliant with UK GDPR and to demonstrate compliance.

Thank you for your assistance.
Kind regards

[Insert Name and Job Title of person signing the letter]

Trust's name:

To comply our arrangements with you under UK GDPR must ensure that you will:

Supplier Requirement	**Confirm consent and process**
Only use the data we provide or that you access from our organisation in accordance with our instructions,	
Ensure that anyone in your organisation understands that and data they have access to or use about our students or staff is confidential and must not be shared with anyone without our prior agreement	
Take all steps to keep the data secure, whether it is paper records, emails, digital or electronic. Please note we reserve the right to ask for evidence and details about how this is done.	
If you sub contract any part of the task, and personal information and data is required by that sub-contractor, you will seek and obtain our consent before proceeding.	
On occasion, we may receive a request to release information that we hold about an individual, whose data you have used or processed on our behalf. Please confirm that in those situations you will co-operate with us and provide all records about the person within a specified timeframe.	
Should there be a data breach, please confirm that you will notify us as soon as you are aware.	
In the event of a breach please confirm that you will co-operate with us to report, manage and recover data that you have also had access to or use.	
In the event of a data breach, what is the process?	
You notify the Trust without undue delay after becoming aware of a personal data breach.	
That you will delete or return (at our choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);	
You will make available to the us all information necessary to demonstrate compliance; allow/contribute to audits (including inspections)	
Please provide answers to the following	
What processes do you have in place for testing the security of your system?	
When was this security system last tested and what was the outcome?	
What is your organisation's strategy for achieving compliance with the UK GDPR?	

Please provide details of your Data Protection/Information Security/Cyber Security Policy as appropriate	

I,..... on behalf of … ..... confirm that the responses above are accurate and agree that completion of this questionnaire forms part of the Trust's supplier due diligence process and does not in itself create a binding data processing agreement.

Signed…….

Dated……...

Role within organisation……...

Appendix 2 to Managing Sub-Contractors and 3rd Parties Process

DRAFT LETTER AND AGREEMENT WITH SUB CONTRACTORS AND 3RD PARTIES

Dear [Insert Supplier Name],

DATA PROCESSOR AGREEMENT

We refer to the arrangement under which you (as the "**Supplier**") provide services to Frank Field Education Trust ("**we**", "**us**", and "**our**"), including the terms and conditions applicable to that arrangement (as updated and amended from time to time) (the "**Terms**").

The UK General Data Protection Regulation (the "**UK GDPR"**) under the Data Protection Act 2018 (the "**DPA**") in regulating the processing of personal data.

As part of our arrangement, we will be forwarding data to you that must be processed in accordance with all applicable Data Protection Laws (including the DPA and UK GDPR).

Article 28(3) of the UK GDPR specifies certain provisions which must be included in contracts between "controllers" and "processors" (such terms are defined in both the DPA and the UK GDPR). As such, this letter sets out the agreement between us to ensure the protection and security of data which we pass to you for processing.

Linked to this, you acknowledge that we are the data controller in respect of any personal data that you process in the course of providing services for us.

AGREEMENT

In consideration for us forwarding to you such data, you agree to comply with all applicable Data Protection Laws and to use your best endeavours to ensure that by your actions you do nothing to compromise Frank Field Education Trust with the applicable Data Protection Laws.
With effect from the date of this letter, you confirm that:

1. The Data Protection Agreement and its Appendix at Annex 1 to this letter ("**Annex 1**") shall form a part of the Terms.

2. The provisions of Annex 1 shall replace any provisions in the Terms which expressly conflict, or are inconsistent, with any provisions of Annex 1. If there is any ambiguity between the provisions of the Terms (excluding this Data Processor Agreement) and this Data Processor Agreement, the provisions of this Data Processor Agreement shall prevail.

3. Except as set out in this letter, the Terms shall remain unchanged and shall continue in force.

NEXT STEPS
Please confirm the categories of personal data and data subjects in the Appendix to the Data Protection Agreement before signing and returning the enclosed copy of this letter (including a full copy of Annex 1) to acknowledge your agreement.

Yours faithfully

Signed ……
Name
For and on behalf of Frank Field Education Trust
Date ……

We agree to the provisions of the UK GDPR Addendum and the variation of the Agreement with effect from the Variation Date on the terms set out above.

Signed ……
Name ……
For and on behalf of ……
Date ……

Annex 1 – Data Protection Agreement

1. Definitions and interpretation

1.1 In this Agreement, unless the context otherwise requires, the following terms shall have the meanings set out below:

(a) "**Trust's Personal Data"** means the Personal Data that you process on behalf of us under or in connection with the Terms;
(b) **"Data Protection Laws"** means all applicable data protection and privacy legislation, regulations and binding codes of practice issued by any DP Regulator, including the Data Protection Act 2018 (the "**DPA"**) and (the **"UK GDPR"**); the Privacy and Electronic Communications (EC Directive) Regulations 2003; and all legislation enacted in the UK in respect of the protection of Personal Data; in each case, to the extent in force, and as such are updated, amended, re-enacted or replaced from time to time;
(c) **"DP Regulator"** means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws;
(d) **"Services"** means the products and/or services provided by you under the Terms and more particularly set out in the background to this Agreement;
(e) **"**Restricted Transfer**"** Restricted Transfer means a transfer of personal data to a separate organisation outside the United Kingdom that is subject to the international transfer requirements of UK GDPR.

UK International Data Transfer Agreement (IDTA) means the transfer agreement approved by the Information Commissioner for UK GDPR transfers where an adequacy decision does not apply.

UK Addendum means the approved UK Addendum to the European Commission Standard Contractual Clauses.;

(f) **"Terms"** means all terms applicable to the legal relationship existing between the parties, including those individually negotiated and subject to written agreements, and under which you and your affiliates are hereafter identified as the "**Supplier**".

1.2 The terms **Data Subject**, **Personal Data**, **Personal Data Breach** and **processing** shall have the meanings set out in the UK GDPR.

2. **Data protection**

2.1 The parties shall comply with the provisions and obligations imposed on them by the Data Protection Laws at all times when processing the Trust's Personal Data in connection with the Terms.

2.2 The details of the processing of the Trust's Personal Data carried out by the Supplier on our behalf are set out in the Appendix to this Agreement and form part of this Agreement (the "**Processing Instructions**").

2.3 Each party shall at all times maintain accurate, complete and up-to-date written records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws and shall make such information available to any DP Regulator on request.

2.4 The Supplier shall:

(a) process the Trust's Personal Data only for the performance of the Services in accordance with the Terms and the Processing Instructions and/or our other written instructions from time to time;
(b) ensure that all of its employees, officers, staff, agents and sub-contractors who have access to the Trust's Personal Data are informed of the confidential nature of the Trust's Personal data and are subject to appropriate contractual obligations of confidentiality when processing such Trust's Personal Data;
(c) implement and maintain technical and organisational measures and procedures to preserve

the confidentiality and integrity of the Trust's Personal Data and ensure an appropriate level of security for the Trust's Personal Data, including protecting the Trust's Personal Data against the risks of accidental, unlawful or unauthorised processing, destruction, loss, alteration, disclosure, dissemination or access;
(d) only appoint a third party (including any subcontractors and affiliates) to process the Trust's Personal Data with our prior written consent;
(e) where the Supplier sub-contracts any of its obligations to a sub-contractor who has been approved by us in accordance with clause 2.4(d), the Supplier shall enter into contractual data

processing provisions with the sub-contractor, equivalent to those in place between the Supplier and us under this Agreement, for the duration of the sub-contractor's Processing of the Trust's Personal Data.
(f) not make a restricted transfer of Trust Personal Data outside the United Kingdom unless authorised by the Trust and an appropriate transfer mechanism and safeguard has been implemented in accordance with UK GDPR requirements.;
(g) inform us without undue delay if the Trust's Personal Data is (while within the Supplier's or its subcontractors' or affiliates' possession or control) subject to a Personal Data Breach or is otherwise lost or destroyed or becomes damaged, corrupted or unusable;
(h) at our sole option, including on termination or expiry of the Terms or any part of them, return or irretrievably delete all the Trust's Personal Data from all of the Supplier's software and/or hardware systems and, if applicable, procure that the Trust's Personal Data is deleted from the software and/or hardware systems of the Supplier's employees, officers, staff, agents or subcontractors (as applicable) and not make any further use of the Trust's Personal Data;
(i) at no additional cost, provide or make available to us and any DP Regulator such information and assistance as is reasonably required to verify, demonstrate or ensure compliance with the Supplier's obligations (and each subcontractor's obligations, if applicable) in this Agreement and/or the Data Protection Laws;
(j) take such steps as are reasonably required to assist us in ensuring compliance with our obligations under Articles 30 to 36 (inclusive) of the UK GDPR;
(k) notify us within two (2) Business Days if it receives a request from a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data;
(l) provide us with such co-operation and assistance as may reasonably be required in relation to any request made by a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data; and
(m) not disclose any Trust's Personal Data to any person or Data Subject other than at our written request or as expressly provided for in the Terms.

2.5 At our request and provided that we shall enter into appropriate confidentiality agreements (as reasonably required by the Supplier), the Supplier shall permit us or our representatives to access any relevant premises, personnel or records of the Supplier on reasonable notice to audit and otherwise verify the Supplier's compliance with its obligations under this this Schedule and the Data Protection Laws.

2.6 If either party receives any complaint, notice or communication which relates directly or indirectly to the processing of the Trust's Personal Data by the other party or to either party's compliance with the Data Protection Laws, it shall as soon as reasonably practicable notify the other party and it shall provide the other party with reasonable co-operation and assistance in relation to any such complaint, notice or communication.

2.7 The Supplier shall indemnify us and keep us indemnified at its own expense against all claims, liabilities, damages, administrative fines, costs or expenses incurred by us or for which we may become liable due to any failure by the Supplier or its Sub-Processors, subcontractors, agents or personnel to comply with any of its obligations under this Schedule or under the Data Protection Laws.

3. **Law and jurisdiction**
3.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and interpreted in accordance with the laws of England and Wales.
3.2 The parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arise out of, or in connection with, this Agreement or its subject matter or formation.