Data Protection Policy (GDPR)

Reviewed	Date of Next Review	Responsibility
September 2024	September 2027	Head of HR

Our Mission:

'To enable young people to live and work without barriers'

Our Values:

- **Teamwork –** we hold ourselves and each other to account and are better when we work together
- **Compassion –** we act with trust, honesty, and kindness in everything we do
- **Inclusion –** we treat each other fairly and with respect
- **Innovation –** we encourage thoughtful, creative, and aspirational ideas
- **Pride –** we encourage each other to be proud of who we are and what we do

Aims

The Senior Leadership Team (SLT) and Trustees of Fairfield Trust (FT) are committed to a Data Protection policy which protects the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

Scope

This policy applies to anyone who has access to personal data and/or is a user of the Trust's IT systems, both in and out of the Trust premises including staff, trustees, volunteers, parents/carers and visitors. This policy applies to all personal data for which the Trust is the Data Controller regardless of whether it is in paper or electronic form and for both staff and learners. Any breach of this policy or of the regulation itself will be considered an offence and the Trust's disciplinary procedures will be invoked.

Compliance

The regulatory environment demands higher transparency and accountability in how organisations manage and use personal data. It also affords stronger rights for individuals to understand and control that use.

The General Data Protection Regulation (GDPR) sets out how the Trust should process and share personal data as data controllers, this includes provisions intended to enhance the protection of student's personal data. For example, the GDPR requires that:

We must ensure that our Trust privacy notices are written in clear, concise language that staff and students will understand.

FT needs to process certain information about its staff, students, parents, carers and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and ongoing employment of staff.
2. The administration of study programmes and courses.
3. Student enrolment and our ongoing commitment to students to safeguarding welfare.
4. Examinations and external accreditation.
5. Recording student progress, attendance and conduct.
6. Collecting fees.
7. Complying with legal obligations to funding bodies and government including local government.

To comply with our various legal obligations, including the obligations imposed by the General Data Protection Regulation (GDPR) FT must ensure that all personal data is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

As a matter of best practice, other agencies and individuals working with FT and who have access to personal information, will be expected to complete a Supplier Assurance statement (available on our website & at Appendix 1*) as well as reading and complying with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request.'

Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

The GDPR also sets out specific rights for Trust students in relation to educational records held within the state education system. These rights are set out in separate education regulations 'The Education (Pupil Information) (England) Regulations 2000'. For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website (www.ico.gov.uk)

Responsibilities under the GDPR

FT will be the 'data controller' under the terms of the legislation – this means we are responsible for controlling the use and processing of personal data. The Trust's staff and associated organisations will be 'data processors' under the terms of the legislation – this means they will process data on behalf of the data controller (FT). The Senior Leadership Team (SLT) are available to address any concerns regarding the data held and how it is processed, held, and used. All staff are responsible for familiarising themselves with and complying with this policy.

SLT are responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging efficient and compliant information handling within the Trust.

SLT are also responsible for ensuring that the Trust's notification is kept accurate. Details of the Trust's notification can be found on the Office of the Information Commissioner's website. Our data registration number is: **Z702315X.**

Compliance with the legislation is the personal responsibility of all staff members of the Trust who process personal information.

Individuals who provide personal data to the Trust are responsible for ensuring that the information is accurate and up to date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the seven principles`. More detailed guidance on how to comply with these principles can be found here (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/#the_principles)

To comply with its obligations, FT undertakes to adhere to the seven principles:

1) **Process personal data fairly, lawfully and in a transparent manner (lawfulness fairness and transparency)**

FT will make all reasonable efforts to ensure that individuals are informed of the purposes for the processing, why we need it and how we will process it, along with any other information which may be relevant.

Individuals have various rights under the legislation including a right to:

- Be told the nature of the information the Trust holds and any parties to whom this may be disclosed.
- Prevent processing is likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Be informed about the mechanics of any automated decision-making process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by automated process.
- Sue for compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

2) Process the data for the specific and lawful purpose for which the data was collected and not further process the data in a manner incompatible with this purpose (purpose limitation)

FT will ensure that the reason for which it collected the data originally is the only reason for which it processes data, unless the individual is informed of any additional processing before it takes place.

3) Ensure that the data is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed (data minimisation)

FT will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant personal data is given by individuals, they will be destroyed immediately.

4) Keep personal data accurate and where necessary, up to date (accuracy)

FT will review and update all data where necessary. The Trust will take every reasonable step to ensure that personal data which is inaccurate will be erased or rectified without delay.

It is the responsibility of the individuals providing their personal data to ensure that it is accurate, and individuals should notify the Trust if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Trust to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary for the purposes for which it is processed (storage limitation)

FT undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation and any other statutory requirements. The Trust will undertake a regular review of the information held and will permanently destroy both paper and electronic records securely in line with the Trust's Retention Guidance.

FT will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (I.E disposal of hard copy files as confidential waste). A log will be kept of records destroyed. The Trust will ensure that any third party who is employed to perform this function will hold the necessary accreditations and safeguards. The Trust has separate retention guidance in place which provides more detail.

6) Process personal data in a manner which ensures appropriate security of the personal data (integrity and confidentiality)

FT will have appropriate security measures in place to protect the personal data it holds. All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. FT will ensure that all personal data is accessible only to those who have a valid reason.

FT will have appropriate security measures in place (this list is not exhaustive):

- Storing all personal data (in hard copy form) in a lockable cabinet with key-controlled access (with the keys then held securely in a key cabinet with controlled access).
- Password protecting all personal data held electronically. Passwords will be in a strong format and updated frequently. Passwords shall not be shared between staff.
- Securely archiving personal data.
- Placing any PCs or terminals, CCTV camera screens etc that show personal data so that they are not visible except to authorised staff.
- Ensuring that PC screens are not left unattended without a password protected screensaver being used. Unattended PCs and devices shall be locked when left unattended.
- Encrypting emails that contain personal/ sensitive data with password protection.

In addition, FT will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed. Job application forms, expression of interest forms and candidate references will be managed via the jobs@ffc.ac.uk email account. An auto deletion rule will be applied to ensure deletion after a certain time period (normally one month).

This policy also applies to staff and students who process personal data 'off-site,' e.g. when working at home and in circumstances additional care must be taken regarding the security of the data.

7) The Trust shall be responsible for and be able to demonstrate compliance (accountability)

The Trust complies with its obligations under the data protection laws including the UK GDPR via the measures set out in this policy including:

- Completing a Record of Processing Activities - Data is collected and processed in an open and transparent manner. The Trust retains a Record of Processing Activities (ROPA) which details the type of data that we process and the grounds upon which we process it. The ROPA can be made available on request.
- The Trust's Fair Processing Notices set out the personal data that is processed and our reasons for this. The Fair Processing Notices can be accessed on our website www.ffc.ac.uk
- Reviewing and auditing privacy measures and compliance
- Reviewing reasons for data breaches
- Completing Data Protection Impact Assessments (DPIAs) where necessary
- Regularly training staff on data protection law

Consent as a basis for processing

FT understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (I.E via the enrolment form or application form) whilst being of a sound mind and without having any undue influence exerted upon them.

Consent obtained based on misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

FT will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and indicate whether the individual needs to consent to the processing.

FT will ensure that if the individual does not give his/her consent for the processing and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Processing Special Categories of Personal Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the UK GDPR. The grounds that we may rely on include:

a) The individual has given explicit consent to the processing of those special categories of personal data for one or more specified purposes
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under the employment and social security and social protection law and research
c) Processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legal y incapable of giving consent
d) Processing is carried out in the course of its legitimate activities by a not-for-profit organisation with a political, philosophical, religious, or trade union aim on the condition that the processing relates solely to its members, or former member who have regular contact with it, and that the personal data are not disclosed outside that body without consent.
e) Processing relates to personal data which are manifestly made public by the individual
f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
g) Processing is necessary for reasons of substantial public interest* but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision- making process. These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018): □ Statutory and government purposes □ Safeguarding of children or individuals at risk □ Legal claims □ Equality of opportunity or treatment □ Counselling Version 4.1 (One West version 2.0) 11 □ Occupational pensions
h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.
i) Processing is necessary for reasons of public interest in the area of public health*.
j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.
   * We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest.

Where the Trust is processing data and expects there is a greater risk to the individuals rights and freedoms, a Data Protection Impact Assessment will be undertaken in order to negate risk and demonstrate compliance with the UK GDPR.

Legal Basis for Processing Criminal Offence Data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions. We do not maintain a register of criminal convictions. We do not retain copies of DS certificates. Information contained within DBS certificates is stored securely within the Trust's Single Central Register and any information contained within the DBS result, is shared with limited staff including those required to carry out the Safer Recruitment Process.

When processing criminal offence data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual
- The processing is necessary for statutory purposes; or
- Consent – where freely given. We acknowledge because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other grounds apply.

Data Breach

In the event of a data breach or near miss, staff will inform the Head of HR so that detailed records can be maintained. The most common examples of data breaches are unlawful loss, alteration, disclosure of personal data, for example, sending an email to the wrong recipient. The Head of HR will assess whether the ICO should be informed within 72 hours as is legally required and/or those data subjects affected by the breach. The culture within the organisation seeks to avoid a blame culture and is key to allowing individuals the confidence to report genuine mistakes. All staff should adopt the approach that they should treat personal data of others with the same care in which they would treat their own. The Data Breach Log will be reviewed regularly and will help identify specific areas of the business who may benefit from further GDPR training and/or support.

Staff will be trained in data protection and internal documents, including this policy. Staff who have a need for additional training will be provided with it. Staff members undertake regular informal discussions on GDPR to ensure key updates are provided where needed. This will include lessons learned from data breaches and near misses, preventative measures to avoid them and other best practice as advised.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the Trust. Any individual wishing to exercise this right should apply in writing to the Principal. Any member of staff receiving a SAR should forward this to the Principal.

In most circumstances, the Trust cannot charge a fee to deal with a request. The Trust reserves the right to charge a reasonable fee for data subject access requests if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

An identification check may be required.

For detailed guidance on responding to SARs including response times, see the detailed ICO guidance available here.

Publication of College Information

FT publishes various items which will include some personal data, e.g.:

- Internal telephone directory.
- Event information.
- Photos and information in marketing materials.

It is FT policy to offer an opportunity to opt-out of the publication of such materials when collecting the information.

Media consent will be sought from both students and staff on a regular basis. Records will be retained to ensure that for those individuals who do not explicitly consent for their image or details to be shared in the public domain, is adhered to. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA.

If the Trust collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Email

It is the policy of FT to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Trust's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the Trust may be accessed by someone other than the recipient for system management and security purposes.

Recording Meetings

The Trust uses AI technology to record certain types of meetings as set out in our Record of Processing Activities, relevant Privacy Notices and Staff Handbook. Consent will be obtained prior to any recording and a transcript or summary will be provided following the meeting. If staff wish to record a meeting themselves, they must make the Trust aware.

CCTV

There are CCTV systems operating within FT for the purpose of safety and security. FT will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation in our CCTV Policy which is available at www.ffc.ac.uk.

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk)which provides further detailed guidance.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact us.

By order of the Board

Tamasin Jones
Head of HR
July 2024

Appendix 1*

GDPR - Summary and Assurance Statement

The UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) came into effect in 2018 and set out seven key principles which dictate our approach to processing personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Our company activities can be referred to as 'Fairfield Trust, 'Fairfield, 'the Trust', 'us' or 'we'.

What is personal data? - Personal data is any information that relates to an identified or identifiable living person (e.g. students, staff member, member of the public, or customer). It generally includes their name, address, phone number, date of birth, place of birth, place of work, dietary preferences, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion or sexuality (as well as other information about them). Information which *indirectly* identifies a person will also be personal data. This would be the case where a single piece of information could not be used to identify a person but could do so in combination with other data or identifiers.

Who needs to comply with the new requirements? - The GDPR applies to both 'Controllers' and 'Processors'. A **Controller** is the person/ organisation which, solely or with others, determines the purposes and means of processing personal data. A **Processor** is the person/organisation which processes the personal data on behalf of the Controller. In most of Fairfield Trust's contracts, Fairfield Trust is the Controller, and the supplier is the Processor.

Why do suppliers need to sign an Assurance Statement? - Where a supplier is processing data on behalf of Fairfield Trust, we must make sure the supplier will implement appropriate technical and organisational measures to comply with the GDPR. For that reason, Fairfield Trust is asking all suppliers to complete and return the attached Assurance Statement.

Until you return the assurance statement it will be deemed that you are agreeing with the GDPR requirement listed on the following pages and are declaring you have suitable measures in place to meet all of the Trust's GDPR requirements.

How to find out more

The Information Commissioners Office can supply more details about processors' obligations. Visit

	GDPR - Supplier Assurance Statement (TO BE COMPLETED & RETURNED)

their website: www.ico.org.uk.

Supplier Name:

GDPR requirements:

	The Supplier confirms that it will:
01.	Act only on written instructions from Fairfield Trust (unless otherwise required by law).
02.	Ensure any processing of personal information is limited to the processing set out in the contract's written instruction.
03.	On the written instruction of Fairfield Trust delete or return all personal information when the Supplier ceases to provide the relevant services.
04.	Ensure that any individuals processing the data are subject to a duty of confidentiality and comply with the Supplier's obligations under GDPR and DPA.
05.	Take appropriate technical and organisational security measures to ensure compliance with the GDPR and DPA.
06.	Only use a sub-processor with the prior written consent of Fairfield Trust and will then ensure that such sub-processor shall comply with these GDPR requirements.
07.	Assist Fairfield Trust to meet its obligations under the GDPR and DPA in relation to allowing data subjects to exercise their rights under the legislation.
08.	Be able to demonstrate (including through records, inspections, audits) to Fairfield Trust at any point, compliance with the GDPR and DPA and will maintain records of data processing carried out on the Trust's behalf.
09.	Report data breaches to Fairfield Trust as data controller without undue delay.
10.	Appoint a Data Protection Officer if the supplier/ supplier's organisation undertakes large-scale data processing.
11.	Only transfer personal data to third countries with Fairfield Trust's prior written consent and in compliance with the GDPR.
12.	Notify Fairfield Trust immediately if it considers that any instructions infringe the GDPR and DPA.
13.	Notify Fairfield Trust immediately if it receives a request from an individual to access the personal data held on them, or if an individual asks to exercise its rights under the GDPR and provide relevant assistance.

Declaration:

Please check one box:

☐The supplier does not process personal data on behalf of Fairfield Trust.

☐The supplier has suitable measures in place to meet all the GDPR requirements set out above and will comply with these when processing data on behalf of Fairfield Trust under any contract, grant or other agreement with Fairfield Trust.

☐The supplier does not yet have suitable measures in place to meet all the GDPR requirements set out above. (Please indicate in the box below which requirements you are currently unable to comply with and describe what steps you will take to ensure compliance and please provide timescales).

Please complete and sign, on behalf of the supplier/supplier organisation, to confirm the declaration above.

Contact name:	
Role in organisation:	
Phone number:	
Email address:	
Postal address:	
Signature:	
Date:	