Data Protection Policy

Date	Revision amendment details	By whom
May 2015	Adopted by TEFAT Board	Trustees
April 2017	Adopted by TEFAT Board	Trustees
Feb 2022	Statutory updates and required revisions reviewed and approved	Ops Group
March 2022	Adopted by TEFAT Board	Trustees
Feb 2025	Review subject to any required statutory updates	Ops Group

Table of Contents

Elliot Foundation Academies Trust Values	3
Purpose	4
Responsibilities	5
What is Personal Data?	5
What activities are regulated by this policy?	6
Why should I worry about complying with this policy?	7
What does “fair and lawful use of Personal Data” mean?	7
What is a Privacy Notice?	8
What is Sensitive Personal Data and what conditions need to be met when processing it?	8
Obligations on processing relevant data and keeping it accurate?	9
Data retention: How long should I keep Personal Data?	9
What are the Individuals’ rights?	10
Requests received for access to Personal Data	10
What kind of security measures might be appropriate?	11
What should I do if I lose Personal Data or I think there is a data security breach?	12
Can I disclose Personal Data to Third Parties?	12
Can I send or transfer Personal Data overseas?	12
What about the use of Personal Data for marketing purposes?	13

Elliot Foundation Academies Trust Values

1. Put children first

a. We trust and value your professionalism
b. We share the responsibility for the learning and welfare of all of our children
c. Our purpose is to improve the lives of children

2. Be safe

a. Don't assume that someone else will do it
b. Look after yourself, your colleagues and all children
c. We are all responsible for each other's safety and well being
d. Discuss any concerns with an appropriate member of staff

3. Be kind & respect all

a. People are allowed to be different as are you
b. Kindness creates the positive environment we all need to flourish
c. This kindness should extend to ourselves as well as to others

4. Be open

a. If you can see a better way, suggest it
b. If someone else suggests a better way to you, consider it
c. We exist to nurture innovators and support those who take informed risks in the interests of children

5. Forgive

a. We all make mistakes
b. Admit them, learn from them and move on

6. Make a difference

a. Making the world a better place starts with you
b. Model the behaviour that you would like to see from others

Related Policies and Documents

Trust IT and Acceptable Use Policy
Trust Freedom of Information Policy
Trust Information Sharing: the 7 Golden Rules
Locally owned Privacy Notices
Privacy Statements and Policies on the Trust website

Definitions

- Where the word 'Trust' is used in this document it refers to The Elliot Foundation Academies Trust.

1. Purpose

The Trust abides by UK data protection laws, including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2018 (GDPR), in its handling of personal information. We aim to ensure our employees are acting in accordance with these laws, the relevant regulatory guidance and best practice.

This policy regulates the way in which the Trust obtains, uses, holds, transfers and otherwise processes personal data about individuals and ensures all of its employees know the rules for protecting personal data. Further, it describes individuals' rights in relation to their personal data processed by the Trust.

2. Responsibilities

TEFAT is the Data Controller for the purposes of DPA and GDPR and has overall control over the purpose and means of the processing of personal data. The Trust Board has overall responsibility for compliance with the statutory requirements.

The Data Protection Officer (DPO) for TEFAT as a whole is the Legal and Governance Director; Jem Shuttleworth (jem.shuttleworth@elliotfoundation.co.uk).

The DPO is responsible for:

- Acting as a contact point for data subjects and the Information Commissioner's Office
- Monitoring the use of personal data across the Trust to ensure internal compliance
- Informing and advising on data protection obligations including leading on the necessary processes for auditing and assessing risk
- Ensuring that adequate systems and policies are in place to support academies to ensure compliance with this policy

Each of our academies is a 'data processor' with a named Local Compliance Officer (LCO) and their details can be found on each academy website. Processors act on behalf of, and only on the instructions of, the relevant controller.

The LCO is responsible for:

- Ensuring locally owned Privacy Notices are updated as required and available on the school website
- Ensuring that where required consent for the disclosure of personal data is obtained; most likely routine consent from parents for the use of photographs for general academy purposes
- Acting as a central point of advice for all staff on data protection matters
- Co-ordinating Subject Access Requests (SAR) for personal data

3. What is Personal Data?

Personal Data is any information (for example, a person's name) or combination of information about a living person, which allows that living person to be identified from that information (for example a first name and an address).

Examples of Personal Data which may be used by the Trust in its day to day business include names, addresses (e-mail and postal addresses), telephone numbers and other contact details, CVs, photos and images, performance reviews, payroll and salary information. The definition also includes opinions, appraisals or intent regarding individuals (eg. employees, job applicants, pupils, parents, personal contacts at suppliers and individual members of the public).

The laws governing how we can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or on paper records (for example, in paper files or filing cabinets).

4. What activities are regulated by this policy?

The Trust processes Personal Data on its employees, pupils, students, parents, carers, agents, the employees of its suppliers and any other individuals, including job applicants and former employees, for a multitude of purposes, including:

- Recruitment
- Employee performance management and professional development
- Payroll and accounting
- Business and market development
- Building and managing external relationships
- Research and development
- Planning and delivering of education and training (including, for example, pupil/student progression rates)
- Staff and student support and facilities management
- Knowledge management
- Research
- Sponsorship funding
- Other purposes required by law or regulation.

When we collect, store, use or erase Personal Data for any of these purposes, this is called processing. If you read, amend, copy, print, delete or send personal data to another entity (whether within your local academy, within TEFAT as a whole or where that entity is not within TEFAT) this is a type of "processing" and is subject to the guidelines set out in this policy.

5. Why should I worry about complying with this Trust policy?

Data protection laws are enforced in the UK by the Information Commissioner's Office (ICO). The ICO can investigate complaints, audit the Trust's processing of Personal Data and can take action against the Trust for breach of the DPA, GDPR and / or other relevant privacy laws.

Such action may include making TEFAT pay a fine and/or stopping the use by the Trust of the unlawfully processed Personal Data, which may prevent the Trust carrying on its education activities.

Entities which are found to be in breach of the DPA, GDPR and / or other privacy laws also often receive negative publicity for the breaches which affects the reputation of the Trust as a whole.

6. What does "fair and lawful use of Personal Data" mean?

One of the main data protection obligations requires the Trust (and its employees) to process Personal Data fairly and lawfully. In practice, this means that the Trust (and each employee) must comply with at least one of the following conditions when processing Personal Data:

- The individual to whom the Personal Data relates has consented to the processing;
- The processing is necessary for the performance of a contract between the Trust and the individual;
- The processing is necessary to comply with a legal obligation placed on the Trust;
- The processing is necessary to protect a vital interest of the individual; or
- The processing is necessary in order to pursue the legitimate interests of the Trust and is not unfair to the individual or otherwise disproportionate to the benefits gained from the processing.

If in any doubt about the fair or lawful use of Personal Data, you should contact the DPO.

If you want to make a new use of any details held by the Trust, you must not do so unless that new use satisfies one of the lawful reasons for processing and it is described in the relevant Privacy Notice provided to an individual (see below). For example if someone provides their details as a parent / carer for pupil support purposes, you may not be able to start sending them marketing emails unless that is covered in an appropriate Privacy Notice and with consent where required from that individual.

7. What is a Privacy Notice?

For data processing to be considered “fair”, when an individual gives the Trust any Personal Data about him or herself, the Trust must make sure the individual knows who the Trust is and what the Trust intends to do with the Personal Data provided to it.

You should give individuals appropriate Privacy Notices when collecting their Personal Data. This means that the Trust has to inform individuals about the processing of their Personal Data at (or before) the time the data is collected. You should therefore check whether there is an applicable Privacy Notice, which covers the processing you intend to carry out for the Trust. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

Privacy Notices must, by law, include information about which data is being collected, who holds the Personal Data, who is the Data Controller, what is the purpose of processing the data, and information on any disclosure to third parties.

Even with consent, or if one of the other lawful reasons for processing applies, the Trust cannot make any use it wants of Personal Data. All the other rules explained in this Policy still have to be complied with. For example, the Trust still has to satisfy the other requirements described below such as making sure the information collected is not excessive. Simply because a person has consented to giving you their information does not override the other requirements of this Policy, or the laws applicable to the Trust. Similarly Personal Data must not be used in a way which would infringe another law. For example for bribery, or racial, age, sexual, or disability discriminatory purposes.

8. What is Sensitive Personal Data and what conditions need to be met when processing it?

Sensitive Personal Data is Personal Data about a person’s race or ethnicity, their health (eg SEN data, child protection plans), their sex life, their religious beliefs, their political views or trade union membership, their physical or mental health or condition, their commission (or alleged) commission of any offence and any proceedings against them in this respect.

Sensitive Personal Data on staff or pupils should not be collected or otherwise processed unless essential to do so. Extra care must be taken with it (in addition to s6 on the normal rules for Personal Data) and it must be kept more securely.

Additional restrictions are placed on top of the lawful reasons for processing mentioned above. For example, consent of the individual has to be explicit (implied consent is not sufficient), and obtained prior to processing any Sensitive Personal Data.

]

TEFAT does not generally seek to obtain Sensitive Personal Data unless:

(i) The individual concerned agrees in writing that TEFAT may do so, on the basis of a full understanding of why TEFAT is collecting the data;

(ii) TEFAT needs to do so to meet its obligations or exercise its rights under employment law; or

(iii) In exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned.

Employees should note that the “legitimate interest” criteria described above is not valid when processing Sensitive Personal Data.

9. Obligations on processing relevant data and keeping it accurate?

The Personal Data (including any Sensitive Personal Data) you collect should be appropriate to, and sufficient for, the relevant purpose(s) you are collecting it for, but not excessive for that purpose(s). Only process the data, which is necessary for the task; minimise your use of Personal Data rather than maximising it. Do not collect and process more Personal Data than you really need. In the end, it simply adds to the Trust’s compliance burden. For example, if you will never telephone someone at home, you do not need their home telephone number.

In addition, you must take care to record and input Personal Data accurately. This is important. There can be serious problems if Personal Data is incorrect. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. If they are not there may be serious problems.

10. Data retention: How long should I keep Personal Data?

The Trust cannot keep or retain Personal Data forever. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). Other records must only be kept while in current use and for a reasonable period afterwards.

As a general rule, when Personal Data is no longer needed by the Trust for the purposes for which it was collected, this Personal Data should be securely destroyed (eg shredded) as soon as practicable.

11. What are the Individuals' rights?

Individuals have certain rights in relation to their Personal Data:

- The right to access Personal Data held about themselves;
- The right to prevent processing of Personal Data for direct marketing purposes;
- The right to have Personal Data corrected;
- The right to compensation for any damage/distress suffered; and
- The right to be informed of automated decision making about them.

Individuals are allowed to withdraw their consent to the Trust's use of their Personal Data at any time. If an individual contacts you to withdraw consent, inform the DPO.

12. Requests received for access to Personal Data

Individuals can also ask for copies of the Personal Data the Trust holds about them and other details about how the Trust uses their Personal Data. Such requests are known as Subject Access Requests (SAR) and may be made in writing or verbally.

On receipt of a request from an individual for access to his/her Personal Data, the Trust (locally or centrally dependent upon the nature of the request) will:

(i) Inform that individual whether the Trust holds Personal Data about him or her;

(ii) Describe the data it holds, the reason for holding the data and the categories of persons to whom it may disclose the data; and

(iii) Provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the data.

If you receive such a SAR there are specific legal rules which must be followed as part of this process. In each case the Trust is under a strict obligation to respond within a specific statutory deadline. Therefore, please contact the DPO for advice.

If you receive a written request for other information about the Trust, it may be a valid request for information under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. In each case the Trust is under a strict obligation to respond within a specific statutory deadline. Therefore, please contact the DPO for advice.

13. What kind of security measures might be appropriate?

The Trust must keep all Personal Data (including Sensitive Personal Data) secure. This means that the Personal Data must be protected against being accessed by other companies or individuals (for example, via hacking), from being corrupted or being lost or stolen. Extra care is needed to secure Sensitive Personal Data because more damage is likely if it is lost.

The Personal Data must also be protected so the wrong people cannot read or use the details. This applies to details in IT systems, e-mails and attachments and paper files. This is why, for example, you have a password and controlled access rights to IT systems. You must comply with the Trust's security procedures (including the IT and Acceptable Use Policy) whenever you handle Personal Data. The Trust relies on you to keep data secure and for data security. Otherwise, there can be serious problems; for example, pupil/student SEN data could be leaked causing significant damage and distress.

If you work away from Trust premises, you must comply with any additional procedures and guidelines issued by the Trust for home working and/or offsite working. You must read these procedures and guidelines before processing any Personal Data away from Trust premises.

The Trust also recognises that adequate security is important where it arranges for outside service providers to process Personal Data on its behalf. Where such arrangements are established by the Trust, service providers must be bound by written contracts to protect the Personal Data provided to them. See the section "Can I disclose Personal Data to Third Parties?" below for more information.

14. What should I do if I lose Personal Data or I think there is a data security breach?

There are potentially significant repercussions for the Trust and the individuals affected arising from a security breach. Where a security breach arises you must:

- Not panic, remember we are where we are!
- Immediately report the details to the DPO providing them with as much information as you have available;
- Follow their guidance on dealing with the security breach and keep them up to date with any further information about it that you become aware of;
- Not approach any individual data subjects, customers, regulators or make any public announcements about the security breach incident without the prior agreement of the DPO

15. Can I disclose Personal Data to Third Parties?

A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. You must not disclose Personal Data to a Third Party outside the Trust unless that disclosure constitutes a lawful reason for processing and satisfies the Privacy Notice requirements.

There are some exceptions to deal with disclosures such as those requested lawfully by police where the information is necessary to prevent or detect a crime. If you receive a request for information about an individual from the government, police or other similar bodies or from journalists or other investigators you should contact the DPO for advice. The application of the relevant exceptions needs careful consideration. The burden is on the Trust to determine whether these apply. Disclosure (however well-meaning and however seemingly authoritative the requestor) without checking risks placing the Trust in breach of several obligations under data protection legislation.

Access to Personal Data must be restricted to those employees of the Trust and Third Parties who need to access it in order to perform their role. You must only process Personal Data where and to the extent you need to see and process it to carry out your job / role properly.

16. Can I send or transfer Personal Data overseas?

The DPA and GDPR contain special rules on whether Personal Data collected in the UK can be transferred to another country. Within the UK, there are restrictions on the transfer of Personal Data outside of the European Economic Area (such a transfer can happen, for example, where Personal Data is e-mailed outside the EEA). This is to make sure the Personal Data remains safe and the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

17. What about the use of Personal Data for marketing purposes?

As with other types of processing, the use of Personal Data for marketing purposes must satisfy the fair and lawful use requirements set out above. This means Privacy Notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent. You therefore should not use Personal Data to contact individuals for marketing purposes (including sole traders and individual members of business partnerships) by email, text or similar unless the individual has specifically and actively consented to marketing use.

It is advisable to check the scope of any marketing consent you are relying upon, particularly if you are sending information relating to Third Parties or contemplating sharing the Personal Data with a Third Party to allow them to do so. If you are obtaining Personal Data from a Third Party for marketing use, then you should check that the consents they have obtained permit the intended processing by the Trust.