Quality Assurance For The Third Sector PLATINUM

Education Futures TRUST
achieving excellence for all

Education **Futures Trust**

Data Protection Policy

Date of previous review: March 2023
Date of update: March 2023
Review date: March 2024
Contact: Chief Executive, Education Futures Trust

Section 1: Aims of this Policy

The Education Futures Trust needs to keep information on its employees, volunteers, service users and Trustees to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection and security procedures. This document also highlights key data protection procedures within the organization.

The safeguards in place are designed to:

- ensure the security and confidentiality of personal information;
- protect against any anticipated threats or hazards to the security or integrity of such information;
- protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any employees, service users, volunteers, trustees and site users.

Section 2: Definitions

2.1 In line with the General Data Protection Regulation principles, the Education Futures Trust will ensure that personal and sensitive data will:

- be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specific and lawful purpose
- be adequate, relevant but not excessive
- be accurate and kept up to date
- not to be held longer than necessary
- be processed in accordance with the rights of data subjects
- be subject to appropriate security measures
- not to be transferred outside the European Economic Area (EEA).

N.B The definition of "Processing" is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

2.2 The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to safeguard personal data.

- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.

- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the GDPR. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.

- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.

- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span in line with GDPR

Section 3: Type of information processed

The Education Futures Trust processes the following types of personal information.

- Information of applicants for posts, including references
- Employee information – contact details, application information, bank account number, payroll information, supervision and appraisal notes
- Volunteer information – contact details, as well as references and application details to include any relevant medical information and details of an emergency contact
- Trustees – contact details and data required by the Charity Commission and Companies House
- Service users – contact details and for some, detailed case notes may be held
- CCTV - images and data may be held for review
- Credit card data .

Personal information may be kept in the following forms:

- Paper based
- Computers based systems.

Groups of people within the organisation who will process personal information are employed staff, and on occasions possibly Trustees.

Section 4: Notification

The organisation will comply with the legal requirements to notify the Information Commissioner that personal data is being processed. For details regarding the Information Commissioner, contact the helpline on 0303 123 1113 or e-mail: casework@ico.org.uk Website: https://ico.org.uk/global/contact-us/helpline/	The need we have for processing personal data is recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires. Interim changes will be notified within 28 days. The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is the Chief Executive.

Section 5: Responsibilities

5.1 Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of the Education Futures Trust, this is the Board of Trustees.

The governing body delegates tasks to the Data Controller which is Chief Executive. The Office Manager will support the Data Controller with the day to day management of this by maintaining and updating the required paperwork.

The Data Controller is responsible for:

- understanding and communicating obligations
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, including any interim changes.

All employed staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Section 6: Policy Implementation

6.1 To meet our responsibilities, staff, trustees and volunteers will:

- ensure any personal data is collected in a fair and lawful way
- explain why it is needed at the start
- ensure that only the minimum amount of information needed is collected and used
- ensure the information used is up-to-date and accurate
- review the length of time information is held
- ensure it is kept safely

- ensure the right people have in relation to their personal data can be exercised.

6.2 We will ensure that:

- everyone managing and handling personal information is trained to do so
- anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do
- any disclosure of personal data will be in line with our procedures
- queries about handling personal information will be dealt with swiftly and politely.

Section 7: Training

7.1 Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms:

7.1 a)

- a copy of this policy along with a verbal explanation from the Data Controller upon induction
- the Declaration at the end of this policy document being signed by every member of staff/volunteer
- new employees/volunteers are reminded that all passwords should be kept private and so must not be shared with other members of staff, or anyone else
- new employees/volunteers are also reminded by their supervisor that data files and documents are kept in locked locations (the details of which will only be provided if needed for recipient's role)
- a "tick list" of information given must be ticked and signed by the recipient at their induction with the office manager as proof of receiving the information and understanding it
- recipients must also sign as proof of receiving any keys, fobs, passwords etc.

7.1 b) General training/awareness raising.

- Staff will be reminded on a regular basis, through supervision and staff meetings, the importance of Data Protection. To ensure everyone has an up to date version of the Policy, this will be recirculated whenever updated.

Section 8: Gathering and checking information

8.1 Before information is collected, we will consider what details are actually required for the organisation's purposes and how long we are likely to require it for.

8.2 We will inform the people whose information is gathered about the following:

- why the information is being gathered
- what the information will be used for
- who will have access to the information (including any third parties).

In most instances, the above will be stated on the information gathering form itself.

8.3 We will take the following measures to ensure that information kept is accurate and up to date:

- regular reminders sent out asking people to check their details (i.e. bank account details, contact numbers, address, in case of emergency contact name and number etc.)

8.4 Personal sensitive information will not be used apart from the exact purpose for which permission was given.

8.5 If the information is required for another purpose, other than that originally stated when permission was first received, but even if the matter is related, consent will be required again in order to use the information

Section 9: Data Security

9.1 The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- lockable cabinets and cupboards, with restricted access to keys
- password protection on personal and sensitive information
- computers set to restrict access to certain, sensitive areas
- where possible, personal data (paper hard copy, laptop) to be kept on site – in appropriate, secure storage when not in use
- when personal data does need to be taken off site (whether paper hard copy or laptop) it must be kept safe and secure, preferably with the member of staff at all times. It must NOT be left in cars or anywhere that could be reasonably seen to be unsafe or unsecure
- laptops and memory sticks must be password protected and encrypted
- data from computers is backed up weekly.

9.2 Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings, and could lead to dismissal.

9.3 The Board and trustees are accountable for compliance of this policy. Any unauthorised disclosure of personal data to a third party by a trustee may result in the trustee being personally liable for any penalty arising from the breach that they have made.

9.4 Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

Section 10: Management of risk

10.1 Access to personal information system is limited to those who have a reason to know such information.

10.2 Each employee is assigned an encrypted laptop with a login and password. Paper files and other legal and paper documents and records are kept in filing cabinets that are locked each night. Only authorized employees have access to these.

10.3 A number of employees have access to personal files and information in order to keep people safe. To further protect personal information, paper documents that contain personal identifying customer information are shredded when the use has ended.

10.4 To reduce risk, employees should not use unsecured devices or memory sticks. Mobile phones should be password protected.

10.4 E-mail communication should be checked prior to sending to ensure that addresses are correct. Sensitive information should not be included in the body of the e-mail, but attached as a passworded document, using the agreed format of passwords. Open group e-mails should not be used: the bcc field should be used to avoid the sharing of e-mail addresses unless written permission has been received.

10.5 Encryption function will be set up on emails and staff will be given instructions on how to use this function and in what context. It will be made clear to staff that email encryption is not a substitute for sending a password protected document.

10.6 Multifactor Authentication is set up for all staff, so they are required to provide additional verification when accessing any new network. This will provide an additional level of security and reduce the risk of cyber attacks which could compromise personal and sensitive data.

Section 11: Data Access Requests

11.1 Anyone whose personal information we process has the right to know:

- what information we hold and process on them
- how to gain access to this information
- how to keep it up to date
- what we are doing to comply with the Act.

11.2 They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

11.3 Individuals have a right under GDPR to access personal data being kept about them on computer and on file. Any person wishing to exercise this right should apply in writing to Carole Dixon, Chief Executive.

11.4 Queries about handling personal information will be dealt with swiftly and politely. We will aim to comply with requests for access to personal information as soon as possible, and will ensure we will respond to your request within one month as required under GDPR. In certain circumstances we may need extra time to consider your request, and this can take up to an extra two months. If this is the case, we will let you know within one month that it needs more time and why.

11.5 A copy of your personal data will be provided free. We would only charge a reasonable fee for administrative costs associated with the request for additional copies or if the request is 'manifestly unfounded or excessive'.

11.6 The following details will be needed to provide the information:

- full name and contact details of the person making the request
- their relationship with the organisation (e.g. former/current member of staff, Trustee, volunteer, service user) to identify or distinguish them from other

people with the same name (account numbers etc.).

- any details or relevant dates that will help it identify what you want.

11.7 We may also require proof of identity before access is granted. The following forms of ID would be requested:

- 1x photo ID, such as passport or photo card driving licence (this must be in date and valid)
- 1x proof of address, such as utility bill or bank statement (this must show the correct, current address and be dated within the last three months)

N.B: If either of these is unavailable, please contact the Chief Executive, or in her absence the Office Manager, to find out what other forms of identification can be accepted.

11.8 You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

11.9 You have the right to ask us to remove your personal information in certain circumstances. You can read more about these circumstances at https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/

11.10 You have the right to restrict or object to us processing your data.

11.11 You have the right to ask that we transfer the information that you gave us from one organisation to another or give it to you. The right only applies if we are processing information based on your consent. If we are processing your information for criminal law enforcement purposes, your rights are slightly different and you can read about this at https://ico.org.uk/your-data-matters/your-right-to-data-portability/.

Section 12: Complaints

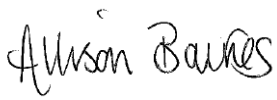
12.1 If you are unhappy with how we have handled your request, you should first follow our Complaints procedure. Please visit our website or request a copy from the Office Manager.

12.2 If you remain dissatisfied you can make a complaint to the ICO.

Section 13: Review

This policy will be reviewed at intervals to ensure it remains up to date and compliant with the law. Data Protection Officer: Carole Dixon, Chief Executive.

Signed: Allison Baines, Chair of the Board of Trustees



Section 13: Declaration

I confirm I have read and understood Education Futures Trust's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a:

Member of staff ☐

Volunteer ☐

Trustee ☐

Signature: ……

Print name: ……..

Date: ……/……/……

Please return this form to the Chief Executive or to the Office Manager. If returning by post, please send to:

Education Futures Trust
The Firs
Elphinstone Road
Hastings
TN34 2AX