Data Protection Policy

Policy Information	
Policy Owner	Chief Operating Officer
Issue Version	V1
Approving Committee	Finance & Audit Committee
Adopted Date	June 2021
Review Cycle	Bi-Annual
Last Review Date	June 2021
Next Review Date	June 2023

Adoption of the Policy

This Policy has been adopted and reviewed by the Trustees of Transforming Futures Trust

Signed **Date: June 2021**

(Chair of Trust)

1. Introduction

This Policy sets out the obligations of the Trust data regarding data protection and peoples' rights in respect of their personal data under the UK General Data Protection Regulation ("UK GDPR").

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Trust, its employees, agents, contractors, or other parties working on behalf of the Trust.

The Trust is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

The Information Commissioners Office (ICO) can investigate complaints, audit the Trust's use or other Processing of Personal Data and can take action against the Trust (and individually in some cases) for breach of these laws. Action may include making the Trust pay a fine and/or stopping the use by the Trust of the Personal Data, which may prevent the Trust from carrying on its educational and associated functions. Organisations who breach one or more laws on Personal Data also often receive negative publicity for the breaches which affects the reputation of the Trust and its activities as a result.

Any breach of or failure to comply with this policy, particularly any deliberate release of Personal Data to an unauthorised third party, may result in disciplinary or other appropriate action.

2. Legal Framework

The EU GDPR is an EU regulation. Therefore, this no longer applies. GDPR has been incorporated into UK law and is know as the 'UK GDPR'. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK only context.

3. Definition

GDPR defines "personal data" as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

4. Data Protection Principles

The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

a. processed lawfully, fairly, and in a transparent manner in relation to the data subject.

b. collected for specified, explicit, and legitimate purposes and not further. processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject;

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. Lawful, Fair, and Transparent Data Processing

UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the person. UK GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- **Consent** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- **Contractual** - processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Legal Obligation** - processing is necessary for compliance with a legal obligation to which the controller is subject.
- **Vital Interests** - processing is necessary to protect the vital interests of the data subject or of another natural person.
- **Public Interest** - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- **Legitimate Interests** - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6. Processing Data

Processed for Specified, Explicit & Legitimate Purposes - The Trust only processes personal data for the specific purposes (or for other purposes expressly permitted by GDPR). The purposes for which we process personal data will be informed to data subjects through the publication of Privacy Notices.

Adequate, Relevant and Limited Data Processing - The Trust will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects.

Accuracy of Data and Keeping Data Up to Date - The Trust shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Timely Processing - The Trust shall not keep personal data for any longer than is necessary taking into account the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase or will be securely disposed without delay.

Secure Processing - The Trust shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Accountability - The Trust holds accountability for Data Protection through an outsourced Data Protection Officer (DPO) service. The Trust shall keep written internal record of all personal data collection, holding, and processing, in the form of a Record of Processing Activities.

7. Data Protection Impact Assessments (DPIA)

The Trust shall carry out Data Protection Impact Assessments (DPIA) when and as required under UK GDPR. Data Protection Privacy Impact Assessments shall be overseen by the Trust's data protection officer and once completed stored in the Trust's GDPRiS system in line with demonstrating accountability.

8. The Rights of Data Subjects

The UK GDPR sets out the following rights applicable to data subjects:

The right to be informed - The Trust shall ensure that the information is provided through the publication and sharing of Privacy Notices. The Trust utilise the DfE's Model Privacy Notices and are published on the Trust and Trust schools' websites.

The right of access; - A person may make a subject access request ("SAR") at any time to find out more about the personal data which the Trust holds about them. The Trust is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). SAR requests are recorded and tracked on the Trust GDPRiS system. The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies

of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

The right to rectification;- If a person informs the Trust that personal data held by the Trust is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

The right to erasure (also known as the 'right to be forgotten'); - Data subjects may request that the Trust erases the personal data it holds about them in the following circumstances where it is no longer necessary for the Trust to hold that personal data with respect to the purpose for which it was originally collected or processed or the data subject wishes to withdraw their consent to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so), The data subject objects to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so); the personal data has been processed unlawfully; or the personal data needs to be erased in order for the Trust to comply with a particular legal obligation.

Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the person's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

The right to restrict processing; - A person may request that the Trust ceases processing the personal data it holds about them. Unless the Trust has reasonable grounds to refuse, all requests shall be complied with and shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

The right to data portability; - Where a person has given their consent to the Trust to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the legal right under UK GDPR to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations). Where technically feasible, if requested, personal data shall be sent directly to another data controller. All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

The right to object; - Where a person objects to the Trust processing their personal data based on its legitimate interests, the Trust shall cease such processing forthwith, unless it can be demonstrated that the Trust's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims. Where a person objects to the Trust processing their personal data for direct marketing purposes, the Trust shall cease such processing forthwith. Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under UKGDPR, 'demonstrate grounds

relating to his or her particular situation'. The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Rights with respect to automated decision-making and profiling. - In the event that the Trust uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, a person has the right to challenge to such decisions under UK GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Trust.

9. Data Protection Measures

The Trust shall ensure compliance with the following when working with personal data:

a. All hardware and mobile devices are encrypted.
b. Digital equipment is disposed of securely.
c. Paper information that contains sensitive and personal data must be disposed. of using a shredder or confidential waste bags.
a. A clear desk policy must be in operation and personal data must be securely locked away when not in use.
b. All hardcopies of personal data, along with mobile devices must be stored securely in a locked drawer or cabinet when not in use.
c. Screens must be positioned appropriately so that personal data cannot be seen by the public and the screen is locked when left unattended.
d. Personal data attached to emails to be avoided where possible. Where it is feasible a link to where the personal data is stored is to be used.
e. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery Mail.
f. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.
g. No personal data should be stored on the computer's hard drive. It must be stored on the Trust network where the data is securely stored and encrypted.
h. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Trust, irrespective of seniority or department.
i. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

10. Accountability – Demonstrating Compliance

The Trust will undertake audits to ensure compliance with this policy and the UK GDPR to ensure that all guidance and support is kept up to date and to ascertain where further guidance and support is needed.

The Trust use GDPRiS – a comprehensive GDPR monitoring and management system. It provides the tools to monitor and demonstrate compliance, with data mapping tools, breach and SAR Management recording and online training and audit functionality.

11. Data Breach Notification

All personal data breaches must be reported immediately to the Headteacher, Academy Data protection Lead or directly to the Chief Operating Officer, who will seek support from the Trust DPO where needed.

The breach is recorded on the Trust GDPRiS system which enables the appropriate notifications and tracking of the breach investigation.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Trust must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

The following steps are undertaken as part of the investigation:

a. Containment and Recovery

The investigation will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment. Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

Advice from experts within and outside the Trust may be sought in resolving the incident promptly and appropriately.

b. Notification

A decision based on the seriousness of the breach will determine subsequent actions. The data protection officer will support and advise on any decision to inform any external organisation, such as the police or other appropriate regulatory body, such as the ICO. The decision to report will be taken by the Executive Team and reported to the Chair of the Finance and Audit Committee.

Where appropriate, Individuals whose Personal Data have been affected by the incident will be notified to enable them to take steps to protect themselves, and where users of Trust information assets have been affected, users will be notified, where appropriate. The notice will include a description of the breach and the steps taken to mitigate the risks.

c. Review

Once the incident is contained, a thorough review of the event will be undertaken. The report will detail the root cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement and recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

Where the breach resulted in notification to the ICO, the report will be signed off by the Executive Committee and submitted to the Trust Finance and Audit Committee.

Appendix 1 – Version Control Amendments

Version No	Date	Summary of Changes