SECKFORD EDUCATION TRUST

POLICY DOCUMENT

Data Protection Policy

Document Owner:	Trust Board
Responsible Trust Committee:	Finance, Audit and Resources
Date Approved:	Michaelmas Term 2021
Review Date:	Trinity Term 2022

APPROVED **Signature (Trust Board):** **Date:**	

Other relevant policies and documents

- Confidentiality Policy
- Freedom of Information Policy
- ICT Policy
- Information Security Policy
- Safeguarding Policy
- Access to Student Records Policy
- Data Protection Acts
- Records Management Policy and Schedule
- Data Privacy Notices

Explanation of Terms

Trust	=	Seckford Education Trust
School(s)	=	schools within the Trust
Personal data	=	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	=	Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence
Criminal convictions		
Processing	=	Obtaining, recording or holding data
Data subject	=	The person whose personal data is held or processed
Data controller	=	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	=	a person, other than an employee of the data controller, who processes the data on behalf of the data controller

1 Purpose of the Policy

This document outlines the Data Protection Policy for the Seckford Education Trust (SET) within the Trust. This policy covers the Trust and all its schools, for which the Trust is the data controller (within the meaning of the Data Protection Act 2018), and as such there is no need for each school to have its own policy.

2 Introduction

The Trust and its schools collect and uses certain types of personal information about staff, students, parents / carers and other individuals who come into contact with the Trust and its Schools, in order that we may provide education and associated functions.

In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), Government agencies and other bodies.

This policy is intended to ensure that personal information must be dealt with properly and securely and in accordance with the Data Protection Act 2018 and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

This Policy does not cover the application of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004: please see our Freedom of Information Policy.

3 Data Protection Act

There are 8 Data Protection Principles as laid down in the 2018 Data Protection Act which must be followed at all times, unless an exemption applies:

- Data must be processed fairly, lawfully and may only be used for the specific purposes
  for which it was collected;
- Personal data shall be obtained only for one or more specific and lawful purposes;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
- Personal data shall be accurate and where necessary kept up to date;
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose;
- Personal data shall be processed in accordance with the rights of data subjects under the 2018 Data Protection Act;

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These include technical measures (such as firewalls) and organisational measures (such as staff training);
- Personal data shall not be transferred to a country outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4 Policy Statement

The Trust is committed to maintaining the 8 principles outlined above. This means that the Trust and its schools will:

- Obtain consent if required for the processing of personal data (please note that consent may not be required if the processing is necessary for the Trust to undertake its obligations to students, and their parents / carers: for example under a contract, or to protect students or others from harm, to fulfil the lawful and legitimate interests of the Trust, or because of some right or obligation conferred on the Trust by law);
- If information is shared we will (except in occasional circumstances where it is lawful and appropriate not to do so) explain to those concerned why, with whom and under what circumstances;
- We will check the quality and accuracy of the information we hold;
- Apply our Confidentiality Policy and Information Security Policy and procedures therein to ensure that information is securely maintained;
- Review the data we hold at regular intervals to ensure personal information is not held longer than is necessary;
- Ensure that when information is properly authorised for disposal this is done securely;
- Ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system;
- We will share personal information with others when it is necessary and legally appropriate to do so;
- We will refer to the Freedom of Information Policy when responding to requests for access to personal information (these requests will be recorded and this information will be reviewed by the Trust Board. An administration fee may be payable);
- We will refer to the Access to Student Records Policy when responding to requests for access to student records (these requests will be recorded and this information will be reviewed by the Trust Board. An administration fee may be payable);
- Train our staff so that they are aware of our policies and procedures;
- This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 2018 and subsequent legislation or regulation.

Sensitive personal data

SET schools may, from time to time, be required to process sensitive personal data about staff, students or parents. Sensitive personal data includes medical information and data relating to religion, race, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the subject will generally be required but there are circumstances where it is not: for example, where necessary to protect the vital interests of individuals, or where required by law (including in the context of employment) or by a statutory authority.

5 Data Protection at the Trust and its schools

5.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the Trust or its schools of a change of circumstances their records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the Trust or its schools will immediately mark the record as potentially inaccurate and until resolved the marker will remain and all disclosures of the affected information will contain both versions of the information.

5.2 Data adequacy and relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Trust and its schools will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

5.3 Authorised disclosures

The Trust and its schools will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Trust and its schools may need to disclose personal data – even sensitive personal data – without explicit consent for that occasion. These circumstances are generally limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations;
- Student data disclosed to authorised recipients in respect of safeguarding (health, safety and welfare);
- Student data disclosed to parents / carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school;
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters; or
- where expressly requested by a relevant authority.

Only authorised and trained staff are allowed to make external disclosures of personal data and internal processing of personal data, in particular sensitive personal information, is handled by appropriate staff on a need-to-know basis. Data used within the schools by administrative staff, teachers and those external agencies with which we work, will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work.

The schools will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse. See Safeguarding Policy for further information.

5.4 Subject Access Request

Individuals have a right to make a 'subject access request' to request a copy of the personal information that we hold about them. To help individuals exercise this right we provide a form on our website. Hard copies of the form can be requested from each school's front office. We ask that SARs are made using the form so that we can ensure that we provide the information requested however subject access requests can also be made verbally or by letter or email.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The user's name;
- A correspondence address;
- A contact number and email address;
- Details about the information requested.

The Trustwill not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the user or another individual;
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- Information contained in adoption and parental order records;
- Certain information given to a court in proceedings concerning the child.

Subject access requests for all or part of the student's educational record will be provided within 40 calendar days.

5.5 Data and computer security

Physical security

Appropriate building security measures are in place, such as alarms, window locks and deadlocks. Only authorised persons are allowed in the network server room. Laptops and printouts are locked away securely when not in use. Visitors to the school are required to

sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied whilst in the building (see Safeguarding and Child Protection Policy).

Electronic data security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files that are password protected. Computer files are backed up daily to a central, secure server.

Procedural security

In order to be given authorised access to the computer network, staff will have to sign an Acceptable Use Policy (see ICT Policy). All staff are trained in their data protection obligations and their knowledge updated as necessary. Printouts as well as source documents containing confidential information are shredded before disposal (see Information Security Policy). The Trust is liable as data controller for the acts of its staff, but individual members of staff should be aware they can be personally liable in law for security failures or wrongful disclosures including under the law of libel, confidentiality, or misuse of private information.

Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

6 Training

Our staff and Trustees are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation or the Foundation's processes make it necessary.

7 The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018. We will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

8 Complaints

Any complaints about this policy from outside the Trust should be made in accordance with the Trust's Complaints Policy. Any other complaints should be brought to the attention of the Head of Schoolof the relevant school in the first instance.

Complaints that are in the public interest and relate to suspected malpractice may be appropriate to raise under the Trust's Whistleblowing Policy.

9 Compliance and Performance Monitoring

The Trust Board will review this policy every two years and ensure that practice across all schools is in line with this policy. Any review will take into account the most up-to-date legislation and guidance.

The Trust has identified a range of Assurance Methodologies as tools by which compliance with policies can be tested. Those most relevant to this policy include:

- External Audit
- Internal Audit
- External Review (by others in the same field)
- Trustee visit/ report
- Random testing by line managers