



Stour Valley Educational Trust

Data Protection Policy

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The data controller	3
5. Data protection principles.....	3
6. Roles and responsibilities	4
7. Privacy / Fair processing notice	4
8. Subject access requests	4
9. Parental requests to see the educational record	5
10. Storage of records	5
11. Disposal of records	6
12. Training.....	6
13. The General Data Protection Regulations	6
14. Monitoring arrangements	6
15. Links with other policies	6

1. Aims

To ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulations 2018.

This policy applies to all data, regardless of whether it is in paper or electronic format and includes CCTV images.

2. Legislation and guidance

This policy meets the requirements of the General Data Protection Regulations 2018, and is based on guidance published by the Information Commissioner's Office and the Department for Education.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

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

4. The Data Controller

The School processes personal information relating to student, staff and visitors, and, therefore, is a data controller. The School delegates the responsibility of data controller to the Data Manager.

The School is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The General Data Protection Regulations 2018 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed

- Personal data shall be processed in accordance with the rights of data subjects under the General Data Protection Regulations 2018
- 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
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The Board of Trustees has overall responsibility for ensuring that the Trust schools comply with its obligations under the General Data Protection Regulations 2018.

Day-to-day responsibilities rest with the Headteacher who will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Privacy / Fair processing notice

7.1 Students and parents

A detailed Privacy Notice for Students is available on the School website.

7.2 Staff

A detailed Privacy Notice for Staff is available on the School website.

8. Subject access requests

Under the Data Protection Regulations 2018, individuals have a right to request access to information the School holds about them. This is known as a subject access request.

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

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

The School will 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 student 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 one month. This timescale may be extended by a further two months where requests are complex or numerous. If this is the case, the individual requesting the data will be informed of this within one month of the receipt of the request and an explanation provided as to why the extension is necessary.

Subject access requests will be provided free of charge.

9. Parental requests to see the educational record

- Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.
- Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.
- For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
- The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.
- The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may not be granted without the express permission of the pupil.
- Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

10. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must ensure the data is secure
- Passwords are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Staff, students or Governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, paper records are shredded and with electronic files being deleted. Internal and external hard drives which are no longer used are destroyed by the Technology department.

12. Training

Staff and Governors are provided with data protection training as part of their induction process. Data protection also forms part of continuing professional development, where changes to legislation or the School's processes make it necessary.

13. The General Data Protection Regulation

The General Data Protection Regulations have replaced the Data Protection Act 1998. Working practices have been reviewed to take into account this legislation and training is provided to all members of staff and Governors, where appropriate.

14. Monitoring arrangements

Trust Business Manager is responsible for monitoring and reviewing this policy.
The Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records annually.
This document will be reviewed by the Trust Board annually.

15. Links with other policies

This Data Protection Policy is linked to the Freedom of Information Publication Scheme and Privacy Notices for students and staff.

Ratified by Trustees	
Date	