

Data Protection Policy and Privacy Notice

First Created: May 2018 – VERSION 1

Version No.	Review Date:	Approval Date:
		27/05/2018
1	26/05/2021	

Policy Agreed	27/05/2018
To be reviewed	3 Yearly
Owner	Dilys Morgan
Designation	Directo



Contents

1. Aims	2
2. Legislation and guidance	2
3. Definitions	3
4. The Data Controller	4
5. Data Protection Principles	5
6. Roles and Responsibilities	7
7. Privacy / Fair Processing Notice	8
8. Subject Access Requests	11
9. Parental Requests to see the Educational Record	12
10. Storage of Records	13
11. Disposal of Records	13
12. Training	14
13. The General Data Protection Regulation	14
14. Monitoring Arrangements	15
15. Links with other policies	15



1. Aims

Our Trust aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

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

2. Legislation and Guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force in 2018.

This policy complies with our funding agreement and articles of association.



3. Definitions

Term	Definition
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: <ul style="list-style-type: none"> • Contact details • 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

Our Trust processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our Trust delegates the responsibility of data controller to the Data Protection Officer. The Trust is registered as a data controller with the Information Commissioner's Office and renews this registration annually.



5. Data Protection Principles

The Data Protection Act 1998 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 Data Protection Act 1998
- 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

Lawful bases for processing data

Consent may not always be the most appropriate lawful reason to use when processing data.

Personal data can be processed without consent if the data is necessary for:

- Fulfilling a contract with the individual
- Compliance with a legal obligation
- Vital interests, i.e. to protect someone's life
- A public task, for example , a public authority that needs to process the information to carry out official functions
- Legitimate interests



5. Data Protection Principles continued

Schools and other public bodies are able to use the ‘public task’ basis for much of the data they process. The ICO’s consent guidance says: If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities.

When processing data on this basis, you must be able to:

- Justify why the processing is necessary to carry out your functions
- Show that the processing is proportionate and that there is no less intrusive alternative
- Ensure that you are fair, transparent and accountable
- Provide “clear and comprehensive” information about how you use personal data, even when you do not ask for consent

As a Multi Academy Trust we are likely to use the lawful bases of Consent and Public Task more often in processing data.



6. Roles and Responsibilities

The Board of Directors has overall responsibility for ensuring that the Trust complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the Headteacher in each academy, or the Deputy Head/Assistant Head in the Headteachers absence. The headteacher 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 Trust academy of any changes to their personal data, such as a change of address.



7. Privacy / Fair Processing Notice

7.1 Pupils and Parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the Trust and each academy is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- name;
- date of birth;
- gender;
- contact information such as email addresses and telephone numbers;
- Parental details
- Permissions for Photographs, trips etc.
- Unique learner number, national insurance, NHS patient number
- Demographic information such as address and post code,
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Social Care information including Child Protection information
- Information regarding entitlement to Pupil Premium
- Details of any medical conditions
- Results of internal and external assessment and externally set tests

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.



7. Privacy / Fair Processing Notice

7.1 Pupils and Parents *continued*

Once our pupils reach the age of 13, we are legally required to pass on certain information to the Local Authority and Youth support service e.g. Connexions, that the academy is in and, if different, the Local Authority and Youth Support service where the pupil resides, which have responsibilities in relation to the education or training of 13-19 year-olds. Parents, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed to the Local Authority and Connexions service by informing the Headteacher of their academy who will then inform the Data Protection Officer for the Trust.

We are required, by law, to pass certain information about pupils to specified external bodies, such as the relevant local authority and the Department for Education, so that they are able to meet their statutory obligations.



7. Privacy / Fair Processing Notice

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, the academies in our Trust. The purpose of processing this data is to assist in the running of the Trust, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as the relevant local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the Trust holds should contact the Headteacher of their academy.



8. Subject Access Requests

Under the Data Protection Act 1998, pupils have a right to request access to information the Trust holds about them. This is known as a subject access request.

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

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

The Trust 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 pupil 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 pupil's educational record will be provided within 15 school days.

If a subject access request does not relate to the educational record, we will respond within 40 calendar days.



9. Parental Requests to see the Educational Record

Parents of children in maintained schools have the right of access to their child's educational record, free of charge, within 15 school days of a request.

However, there is no equivalent legal right for parents of pupils attending an academy, so parents of pupils in The Sovereign Trust academies do not have an automatic right to access their child's educational record. The Trust 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).

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.



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 sign it in and out from the office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils, where appropriate, are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or directors/committee members 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, 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.



12. Training

Our staff and directors/committee members 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 Trust's processes make it necessary.

13. 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 directors and committee members where appropriate.



14. Monitoring Arrangements

The Data Protection Officer is responsible for monitoring and reviewing this policy.

The Data Protection Officer checks that the Trust complies with this policy by, among other things, reviewing Trust records on a regular basis.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the Board of Directors.

15. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

