

Data Protection Policy

Approval Date	04/01/2016
Version	1.0
Review period	Annually
Review date	03/01/2016



Contents

1 Introduction 3

2 Principles 3

3 Satisfaction of principles 4

4 The Trust’s Designated Data Controller 4

5 Subject access 4

6 Employee responsibilities 4

7 Data security 5

8 Rights to access information 5

9 Publication of The Sovereign Trust information 5

10 Subject consent 5

11 Retention of data 5

12 Supporting material 5

13 Relationship with existing policies **Error! Bookmark not defined.**

1 Introduction

The Sovereign Trust (The Trust) is required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. The Trust recognises the importance of the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.

The types of personal data that The Trust may require include information about: current, past and prospective employees; current and past Pupils, Members; Trustees; suppliers and others with whom it communicates. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

The Trust fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. **Employees** and **any others** who obtain, handle, process, transport and store personal data for the Sovereign Trust must adhere to these principles

2 Principles

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for those purposes;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose;
6. Be processed in accordance with the data subject's rights;
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or
8. And not be transferred to a country or territory outside the European Economic
9. 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.

3 Satisfaction of principles

In order to meet the requirements of the principles, **the Trust and All Staff** will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- take the appropriate technical and organisational security measures to safeguard personal data;
- and ensure that personal data is not transferred abroad without suitable safeguards.
- Compliance with this policy will in turn facilitate compliance not only with information-related legislation (specifically FOI 2000) but also with other legislation or regulations (including audit, equal opportunities and research ethics) affecting the institution

4 The Trust's Designated Data Controller

The **Board of Trustees** has overall responsibility for this policy. The **Trust Business Manager** is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Trustees. The Trust Business Manager may be contacted at:

The Sovereign Trust
Manor Academy
Manor Avenue
Sale
Greater Manchester
M33 5JX

5 Subject access

All individuals who are the subject of personal data held by the Trust are entitled to:

- Ask what information the Trust holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the Trust is doing to comply with its obligations under the 1998 Data Protection Act.

6 Employee responsibilities

All employees are responsible for:

- Checking that any personal data that they provide to the Trust is accurate and up to date.
- Informing the Trust of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the Trust may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, employees may collect information about other people (e.g. about Health care professional details or personal circumstances, or about employees in their Academy), they must comply with this Policy

7 Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

8 Rights to access information

Employees and other subjects of personal data held by the Trust have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the Trust's Business Manager.

The Trust reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.

The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed form and fee unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

9 Publication of The Sovereign Trust information

Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on staff contained within externally circulated publications. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Trust's Business Manager.

10 Subject consent

The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate The Trust policies, such as health and safety and equal opportunities.

11 Retention of data

The Trust will keep some forms of information for longer than others. **All staff** are responsible for ensuring that information is not kept for longer than necessary.

12 Supporting material

The purpose for holding personal data and a general description of the categories of people and organisations to which we may disclose it are listed in the Data Protection register. This information may be inspected or obtained from the Information Commissioner's Office.