Southend High School for Girls

Data Protection Policy

Last reviewed: March 2018

Governor Policy No 13S.	Author: Bursar	Authorised by: Board of Governors
Data Protection Policy	Date first issued 11/09/2014	Page 1 of 5.

Reviewing authority: Board of Governors / Committee

Date for review	Reviewed by	Reviewed by Board	A	B	C	Date of new edition
Sept 14.	SC	11.09.2014	*			
March 2018	SC	27.03.2018				27.03.2018

A = accepted with no amendments

B = accepted with amendments

C = new edition created

DATA PROTECTION

Introduction

1.1 The **Data Protection Act** (DPA) 1998 became law in March 2000. The primary aim of the Act is to give legal rights to "**Data Subjects**" in respect of personal data processed about them by "**Data Controllers**".

1.2 From 25th May, 2018 the EU's **Data Protection Regulations** (GDPR) will also become mandatory for countries operating within the European Union. The GDP Regulations are very similar to those of the DPA although the penalties for breaches are more severe.

1.3 Southend High School for Girls Academy Trust is a **Data Controller** and **Processor** for the purposes of the Data Protection Act. The school is registered with the Information Commissioners Office (ICO) with Registration No Z2544750.

The school necessarily collects data about our students and their parents (or Carers), and staff as well as for suppliers, and holds it in electronic and/or paper format in secure locations. We may also receive information about students from their previous school, the Learning Records Service and the Consortium of Selective Schools in Essex.

We use data held about pupils staff and suppliers for compliance with the legal obligations to which the Academy is subject and for the legitimate interests pursued by the Academy. (EU GDPR Article 6:C and EU GDPR Article 9:f).

In registering a student at the Academy, explicit consent to the processing of data to support the education of the student is given by parents, (and by students on reaching age 18). (EU GDPR Article 9:2). In registering a member of staff at the Academy, explicit consent to the processing of data to support the employment of that individual is obtained from them. With effect from 25th May, 2018 data will be processed in accordance with the special category applicable to education specified in the GDPR.

Processing is necessary to protect the interests of students and staff and is carried out in the course of legitimate educational activities with appropriate safeguards.
(EU GDPR Article 9: C and EU GDPR Article 9: D).

1.4 It is the policy of the school that all personal information will be dealt with lawfully and respectfully, whether it is collected, recorded and processed on paper, electronically, on or in, any other material. The DPA prescribes how the School must look after that information.

Policy Statement

2.1 The lawful, fair and correct processing of personal information by the School is vital to enable it to operate efficiently and to maintain the confidence of the public.

2.2 To this end the School fully endorses and adheres to the principles of data protection as detailed in the DPA and GDPR and has adopted the Records Management Society's (RMS) recommendations in respect of data and document retention periods and custody. A copy of the latest version of the RMS's "Retention Guidelines for Schools" will be maintained on the "G" Drive of the school's ICT Network and therefore be accessible to all staff. Staff will be reminded of their responsibilities under this policy, and the law, on a regular basis.

2.3 The school will not use data held about students and their parents or carers for marketing purposes without first obtaining parental consent to do so. Parents will be invited to agree to receive school newsletters in which forthcoming school events are listed and given a choice as to whether they wish to receive such correspondence by e:mail or letter. Correspondence promoting school events can only be sent to parents who opt-in to

receiving these notifications. Parents will be provided with the ability to “unsubscribe” from receiving electronic versions of the school’s “Highlights” newsletter and Gazette.

2.4 The school is committed to using third parties and software suppliers who are compliant with GDPR.

The Eight Data Protection Principles

3.1 The DPA consists of 8 enforceable principles for good information handling and practice with which Data Controllers must comply.

These are that personal data shall:

- be processed fairly and lawfully,
- be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- be accurate and, where necessary kept up to date;
- not be kept for longer than is necessary for that purpose or those purposes;
- be processed in line with the rights of the data subjects under the 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;
- not be transferred to a country outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

Compliance with the Principles

4.1 The School will, through strict application of criteria and controls:

- Adhere fully to conditions regarding the fair collection and use of all information.
- Meet its legal obligations to specify the purposes for which information is used; including specific requirements that must be met to ensure fair and lawful sharing of personal data both internally and externally by issuing and publishing a Data Protection Privacy Statement.
- Collate and process relevant personal information, and only to the extent that it is needed to fulfil operational requirements or to comply with any legal or statutory obligation.
- Ensure the quality of information used.
- Apply stringent checks to determine the length of time information is held.
- Ensure that individual data subjects and the public are able to fully exercise their rights under the Act and GDPR. These include having the right of access to their personal information, the right to be informed that processing is undertaken, the right to be able to correct, block, remove or destroy information which is inaccurate or contains expressions of opinion based on inaccurate information and in certain circumstances prevent processing or disclosure of information.
- Ensure compliance with the School’s ICT Policies, including the ICT Acceptable Use Policy.
- Ensure that all staff are aware of this policy and understand the need for Encryption of laptop computers storing private data, and implement procedures to manage breaches of Data Protection in line with Principle 7.
- Ensure that personal information is not transferred outside the European Economic Area without suitable and adequate protection, and only to countries employing adequate internationally recognised controls.
- Ensure that the School’s Registration with the Information Commissioner’s Office remains up to date and accurate.

Management of Data Protection

5.1 The School will ensure that:

- there is someone with specific responsibility for data protection. Currently the nominated person is the Bursar. The Pay & Personnel Committee is corporately responsible for managing Data Protection and to provide advice on aspects of this policy to data owners in the School;
- the Bursar and Headteacher disseminate best practice across all Faculties and the Bursar deals with all Subject Access Requests in line with the Data Co-ordinators' Roles and Responsibilities Guidance;
- all staff who manage and handle personal information will be held responsible for adhering to good data protection practice;
- all staff managing and handling personal information are adequately and appropriately trained and supervised;
- back-up tapes used to store copies of data are kept for between one and two months only and are then overwritten or destroyed;
- all queries on handling personal information are dealt with promptly and courteously;
- methods and documentation for handling personal information are clear and readily available;
- methods of handling personal information are regularly assessed and evaluated;
- performance of handling personal information is regularly assessed and evaluated;
- the way that personal information is managed is reviewed and audited;
- all staff and students are made aware of the conditions under which computers in the school may be used and that they sign an "Acceptable Use Policy" agreeing to the terms;

Complaints and Breaches of Data Protection

6.1 The School will take the following steps to enforce this Policy and deal with any complaints by following the school's Complaints Procedure Policy.

- Managers are to ensure that all staff are aware of the importance of protecting data in line with the terms and conditions of their employment. The Human Resources (HR) Manager will advise and support Department Managers with any disciplinary action that needs to be followed.
- Potential breaches of Data Protection legislation will be dealt with in accordance with the applicable law.
- The School's Senior Leadership Team (SLT) must apply a fair and consistent approach to the recording and management of all Data Protection breaches, including notification of breaches to affected individuals (the data subjects). In each case, a risk assessment of the consequences of the breach, conducted in line with guidance from the ICO will be carried out in accordance with the existing HR investigation procedures.
- The Headteacher will be responsible for notifying an affected individual of any data security breaches that affect them (Principle 7) in line with advice from the ICO.
- The Headteacher and HR Manager will follow established disciplinary procedures for each breach where a member of staff or department is found to be accountable for the breach of this policy. Responsibility may then transfer to the relevant line manager to investigate, with support from the HR Manager as appropriate. Any disciplinary action must be taken in line with the Staff Discipline Policy.

Monitoring of this Policy

7.1 This Policy will be reviewed annually but may be revised sooner should the need for this arise. Implementation of the policy will be overseen by the executive SLT and be reported to Governors on an exceptions basis.