

SOUTH EASTERN EDUCATION AND LIBRARY BOARD

Data Protection Policy

Introduction

The South Eastern Education & Library Board recognises and accepts its responsibility as set out in the Data Protection Act 1998 and sub-legislation contained therein. The Board, as a Data Controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information.

This policy statement applies to all Board members and employees, and individuals about whom the Board holds and uses personal information, as well as other partners and companies with which the Board undertakes its business.

Scope

The South Eastern Education and Library Board needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective employees, pupils, students, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 1998.

We regard the lawful and correct treatment of personal information by the Board as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The Board wishes to ensure that it treats personal information lawfully and correctly.

To this end we fully endorse the obligations of the Act and adhere to the Principles of data protection, as enumerated in the Data Protection Act 1998.

The following paragraphs provide a brief aid to the Data Protection Act 1998.

1. Main Provisions of the 1998 Legislation

(a) Ensuring Personal Data is registered with the Data Protection Commissioner. The Board must supply certain information to the Commissioner who maintains a public register of what sort of information organisations process, where it gets it from and what it does with it.

(b) Observing the eight Data Protection Principles (more detail below).

- (c) Allowing the data subject to exercise his/her rights and have right of access to their personal information, what is held, how it is processed, to whom it is disclosed and to be told of the logic behind automated decisions. Such requests must be complied within 40 days and the maximum chargeable fee is £10.

2. Definitions

Data Controller	Any individual or organisation who controls personal data, in this instance the Board.
Personal Data:	Information held on a relevant filing system, accessible record or computerized record (as well as digital audio or video equipment), which identifies living individuals.
Sensitive Personal Data:	Personal data relating to an individuals race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.
Relevant Filing System:	Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records, microfiches.
Data Subject:	An individual who is the subject of the personal data, for example, employees, pupils, claimants etc.
Processing:	Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

3. Data Protection Principles

Specifically, the Principles require that personal information:

- (a) shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
- (b) shall 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;
- (c) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- (d) shall be accurate and, where necessary, kept up to date;
- (e) shall not be kept for longer than is necessary for that purpose or those purposes;
- (f) shall be processed in accordance with the rights of the data subject under the Act;

and that:

- (g) 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;
- (h) shall not be transferred to a country or territory 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.

Commitment

The South Eastern Education and Library Board will, through appropriate management and application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, block or erase information which is regarded as erroneous);
- take appropriate technical and organisational security measures to safeguard personal information; and
- ensure that personal information is not transferred abroad without suitable safeguards.

Compliance

In addition, the South Eastern Education & Library Board will take steps to ensure that:

- there is someone with specific responsibility for data protection in the organisation. (Currently, the nominated person is the I.S. Manager, Corporate IT Services);
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;

- methods of handling personal information are clearly described;
- a regular review and audit is made of the way personal information is managed;
- methods of handling personal information are regularly assessed and evaluated;
- performance of handling personal information is regularly assessed and evaluated; and
- disseminate to employees information on good practice in respect of handling, using and storing personal information.

A copy of this policy statement will be issued to all employees. It will be reviewed annually, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

The Board also operates a formal Complaints Procedure which employees and the public can avail of in respect of this policy.

Authorised by: _____
Chief Executive

Date: _____

South Eastern Education & Library Board

DATA PROTECTION POLICY

ORGANISATION

Senior Management

The Chief Executive and Senior Officers have overall responsibility for all matters relating to the obligations under the Data Protection Act 1998, and for ensuring all persons employed by the Board are aware of their duties in respect to the handling, usage and storage of personal information, including inclusion in the Risk Assessment process.

In the discharge of these duties the following applies:

Service & Unit Managers

Each manager has a duty to adhere to the eight Data Protection Principles in relation to the information within their area of responsibility, as well as other Board information to which they have access as part of performing their duties. Adherence to the Principles involves regular review of collecting, recording, handling, storing and releasing personal information to both internal and external parties according to the Board's notification to the Information Commissioner. Each manager must ensure that staff are made aware of their role and responsibility in this area, and regularly review procedures, and the accuracy and relevancy of information held and requests received for access to information.

Board Employees

Every Board officer has a legal duty to take care of personal data and thus comply with the Data Protection Act 1998. Employees must comply with policies and procedures issued in respect of personal information and take care in the collection, recording, handling, storing and releasing personal information during the course of their duties.

South Eastern Education & Library Board

DATA PROTECTION POLICY

Offences

Every Board officer has a legal duty to take care of personal information and to comply with the Data Protection Act 1998.

The consequences of breaching the Data Protection Act may be extremely costly to both you and the Board.

Officers could not only find themselves facing disciplinary action or dismissal but also criminal prosecution for which they may be fined.

The Board may in addition face a civil action, which may mean we will have to:

- ❑ Revise procedures;
- ❑ Face a claim for compensation from individuals; or
- ❑ Face action by the Information Commissioner if the Data Protection Principles have been breached. This could lead to the Board having to delete important data, which could seriously impact our services.