

Southend High School for Boys



Data Protection Compliance Statement

April 2023

Data Protection Officer: dpo@shsb.org.uk

This statement summarises Southend High School for Boy's approach to compliance with The Data Protection Act 2018 (the Act) and will be used to ensure compliance, and as evidence of compliance for data protection inspections and audits. Compliance is vital to protect the staff, students, parents, volunteers and customers of the School from the consequences of the misuse of their personal data. The School is aware of the potential consequences of non-compliance for individuals, which could be personal or financial, and for the School, in terms of its reputation, and the notices and financial penalties which could be imposed by the Information Commissioner's Office.

Definitions

1. Personal data – data identifying a living individual e.g. contact details, appearance
2. Special categories of personal data – sensitive data e.g. ethnicity, sexuality, health, biometric data
3. Data Subject– a living person, by law, at least 13 years old, who is the owner of the data
4. Privacy Notice – declaration of legal reasons for processing data and how it is used
5. Data Controller – responsible for ensuring that we act according to the Act and our Privacy Notices
6. Rights of the Data Subject– security, accuracy, access, appropriate use and destruction
7. Subject Access Request – the means by which people can access their personal data
8. Data Security – adequate protection of personal data
9. Data Breach – the disclosure, corruption or destruction of personal data
10. Data Protection Impact Assessment – process to help minimise the data protection risks of a project
11. The School – Southend High School for Boys
12. ICO – Information Commissioner's Office - the United Kingdom's independent body set up to uphold information rights.
13. DPO – Data Protection Officer – independent expert in data protection who assists in monitoring and demonstrating internal compliance, informs and advises on data protection obligations, Data Protection Impact Assessments (DPIAs) and acts as a contact point for the Information Commissioner's Office (ICO).

Scope of Information Processed

Personal data, including special category data, processed by the School is detailed in our Privacy Notices:

[Privacy Notice for Parents and Students](#)

[Privacy Notice for Volunteers \(including Governors\)](#)

[Privacy Notice for Staff and Job Applicants](#)

[Privacy Notice for Lettings](#)

Rights of the Data Subject

The rights of the data subject are as follows:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The school is aware of the rights of data subjects and works to ensure that it protects these rights by acting in accordance with the points below.

1. Data Protection Principles

The school is committed to processing data in accordance with its responsibilities under the the Act.

Article 5 of the Act requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Act in order to safeguard the rights and freedoms of individuals; and

- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. General provisions

- a. This policy applies to all personal data processed by the school.
- b. This policy shall be reviewed by the Data Protection Officer at least annually and any proposed amendments directed to the Headteacher; updates will be reported to the Governing Body.
- c. The school shall remain registered with the Information Commissioner's Office as an organisation that processes personal data.
- d. Data Controllers will be appointed for the areas of parent, student and volunteer data, staff data, and information security. The Headteacher is the overarching Data Controller for the school.
- e. The school shall appoint a Data Protection Officer who will report to the school's Governing Body and work with the school's Data Controllers to ensure compliance.
- f. All recommendations made by the Data Protection Officer will be logged in the school's Recommendation Log.
- g. The Data Protection Officer will perform audits each school term and report concerns, recommendations and actions taken to the school's management team and the Governing Body.
- h. The Governors will nominate a Governor to have a special interest in data protection, who will act as the Link Governor for the Data Protection Officer on the school's Governing Body.

3. Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the school shall maintain registers of the data it collects along with its retention rules.
- b. The registers will be reviewed annually.
- c. Individuals have the right to access their personal data and any such requests made to the school shall be dealt with in a timely manner, according to the school's Subject Access Request Procedure. All requests will be recorded in the school's Subject Access Request Log.

4. Lawful purpose

- a. All data processed by the school must be done in accordance with one of the lawful bases as defined in the Act.
- b. The school shall note the appropriate lawful basis in its registers and Privacy Notices.
- c. Privacy Notices will be made available at the point of data collection.
- d. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- e. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the school's systems.

5. Data minimisation

- a. The school shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- b. Collection of information is audited annually to ensure it is reflected accurately in the school's Privacy Notices and that all information collected is necessary according to the lawful bases.

6. Accuracy

- a. The school shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
- c. Owners of personal data are prompted to update their information annually.

7. Archiving/removal

- a. To ensure that personal data is kept for no longer than necessary, the school shall put in place a retention schedule for each area in which personal data is processed and review this process annually.
- b. The retention schedules shall consider what data should/must be retained, for how long, and why.
- c. Data subjects can request the erasure of their data. The school will comply with these requests, unless unable to do so for legal reasons.

8. Security

- a. The school shall ensure that personal data is stored securely using modern software that is kept up to date.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.
- d. Appropriate backup and disaster-recovery solutions shall be in place.
- e. Staff shall be made aware of the Data Protection Principles and the steps to take in the event of a breach, or if they receive a Subject Access Request.

9. Breach

- a. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the school shall promptly assess the risk to people's rights and freedoms and, if appropriate, report this breach to the ICO.
- b. The school will follow its Breach Procedure.
- c. The Data Protection Officer will be advised of breaches, monitor the school's response, advise on whether reporting to the ICO is appropriate, and record all breaches in the school's Breach Log.