Sackville School
Data Protection Policy

Reviewed by: Pete Cowlin **Date adopted:** March 2025
Next Review Date: March 2027

Executive Summary
New policy framework updated from The Key

1. Introduction

1.1 Purpose of the Policy

This Data Protection Policy outlines the measures the school takes to ensure that personal data is collected, used, stored, and disposed of securely and in compliance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The policy provides staff, pupils, parents, and third parties with clear information regarding how the school processes personal data and the rights individuals have under data protection legislation.

1.2 Scope of the Policy

This policy applies to all processing of personal data carried out by the school, including that of current, past and prospective pupils, parents and carers, staff, governors, contractors, volunteers, visitors, and service providers. It covers all forms of data processing including paper-based record keeping and electronic systems. The policy applies to all staff, including temporary and part-time personnel, and to any third parties who process data on behalf of the school.

1.3 Legislative Context

The school is committed to complying with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education Acts 1996 and 2002
- Equality Act 2010
- The Children Act 1989 and 2004
- Working Together to Safeguard Children (2018)The policy also aligns with guidance from the Department for Education (DfE) and the Information Commissioner's Office (ICO), including the DfE's 'Data protection: a toolkit for schools.'

2. Roles and Responsibilities

2.1 Governing Body

The governing body holds overall responsibility for ensuring the school complies with data protection legislation. It oversees the effectiveness of this policy and ensures systems are in place to identify and manage data protection risks.

2.2 Headteacher

The Headteacher holds executive responsibility for data protection compliance within the school and ensures that staff receive appropriate training and support to implement the policy in their daily duties.

2.3 Data Protection Officer (DPO)

The school has appointed a DPO with the duties set out in Article 39 of the UK GDPR. The DPO monitors compliance, oversees data protection impact assessments (DPIAs), advises on data protection matters, and serves as the point of contact with the ICO.

2.4 All Staff

All employees must comply with this policy and attend data protection training as required. Staff should immediately report any data protection concerns or breaches to the DPO.

2.5 Third-Party Processors

Third parties processing personal data on the school's behalf must do so under a formal written contract in accordance with Article 28 of the UK GDPR. The school ensures due diligence checks are conducted on all data processors.

3. Legal Bases for Processing Personal Data

3.1 Lawful Bases under Article 6

The school processes personal data using the following legal bases:

- **Public task**: Processing necessary for performing a task in the public interest or in the exercise of official authority.
- **Legal obligation**: Processing necessary to comply with legal obligations (e.g. safeguarding).
- **Vital interests**: Processing data to protect the vital interests of the data subject or another individual (e.g. emergencies).

- **Consent**: Used when no other lawful basis applies, particularly for activities such as school photography or marketing.

3.2 Special Category and Criminal Offence Data

Special category data (e.g. health, ethnicity, biometric data) is processed under Article 9 with an additional condition from Schedule 1 of the Data Protection Act 2018. Criminal offence data is processed in accordance with Article 10 of the UK GDPR, only when authorised by law.

4. Data Collection, Use and Sharing

4.1 Categories of Personal Data Held

Personal data collected and processed includes:

- **Pupil data**: Name, date of birth, address, contact details, attainment, behaviour, medical and SEN information, safeguarding notes.
- **Staff data**: Contact details, employment records, payroll information, DBS checks, professional development records.
- **Parent/carer data**: Names, addresses, contact details.
- **Other individuals**: Visitor logs, volunteers, governors, external providers.

4.2 Why the School Collects and Processes Data

The school processes personal data for specific purposes, including:

- Delivering the curriculum and monitoring pupil progress
- Providing pastoral care and safeguarding pupils
- Managing recruitment, contracts and staff development
- Facilitating communication with parents and carers
- Meeting statutory obligations (e.g. safeguarding, census returns)

4.3 Data Sharing

The school shares personal data securely with:

- Local authorities
- The Department for Education (DfE)
- The NHS and relevant healthcare professionals
- Social services and other safeguarding partners
- Educational providers and examination boards

- External data processors who provide services to the school

Data sharing is conducted under a clear legal basis and is proportionate and necessary.

4.4 Data Sharing Agreements

Written agreements are in place with third-party processors to ensure compliance with data protection legislation. These include clear roles, responsibilities, and data security expectations.

5. Data Subject Rights

5.1 Individual Rights under UK GDPR

All individuals whose data is held by the school have the following rights:

- Right to be informed about how their data is used
- Right of access to their personal data
- Right to rectification of inaccurate data
- Right to erasure (‘right to be forgotten’) in certain circumstances
- Right to restrict processing
- Right to data portability
- Right to object to data processing
- Rights regarding automated decision-making and profiling

5.2 Subject Access Requests (SARs)

Individuals may request access to their personal data. Requests should be submitted in writing to the school. The DPO will coordinate the response within one calendar month. Additional verification may be required. Parents can request access to their child’s personal data provided that it does not conflict with the child's best interests.

6. Data Accuracy and Security

6.1 Accuracy of Data

Staff are required to check and update data regularly and correct inaccuracies without undue delay. Pupils’ contact and medical records are reviewed annually.

6.2 Security Measures

The school implements appropriate technical and organisational measures to protect personal data:

- Secure storage (locked filing cabinets, password-protected files)
- Controlled and limited access to sensitive data
- Use of encrypted emails for sensitive communications
- Regular back-ups of data
- Anti-virus and firewall protection

6.3 Use of Portable Devices and Cloud Services

Staff must follow school policies on mobile devices and remote working. Personal data must not be stored on USBs or unencrypted personal devices. Cloud services are assessed for data security compliance.

7. Retention and Disposal of Records

7.1 Retention Schedule

The school follows the IRMS 'Information Management Toolkit for Schools' for data and document retention. Different categories of data have defined retention periods based on legal requirements and school needs.

7.2 Secure Disposal

Data no longer required is disposed of securely. Paper records are shredded or incinerated. Digital records are permanently deleted using appropriate software. Disposal is recorded and monitored.

8. Data Breach Management

8.1 Definition of a Breach

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

8.2 Reporting of Breaches

All staff are required to report data breaches or potential breaches immediately to the DPO, who will assess the significance and impact of the breach.

8.3 Breach Response Plan

The school maintains a breach log and will:

- Contain and recover the breach

- Assess risks to individuals
- Notify the ICO within 72 hours if the breach poses a risk to rights and freedoms
- Notify affected individuals where required
- Take remedial action to prevent recurrence

9. Training and Awareness

9.1 Induction Training

All new staff receive induction training, which includes a section on data protection and their responsibilities.

9.2 Ongoing Training and Refreshers

Annual refresher training is delivered to all staff to ensure continued compliance and raise awareness of current issues.

9.3 Role-Specific Training

Staff handling large volumes of personal data such as the SENCO, DSL, and administrative staff receive targeted training. The DPO undertakes accredited CPD in data protection.

10. Monitoring and Review

10.1 Monitoring Compliance

The DPO conducts regular data audits to assess practice and ensure that data protection controls are effective. Risk assessments are conducted when new data systems are introduced.

10.2 Policy Review

This policy is reviewed annually by the Headteacher and Governing Body. Updates are made in response to changes in legislation, guidance, or as a result of audit findings.

11. References and Supporting Documents

- Data Protection: a toolkit for schools (DfE)
- UK GDPR and Data Protection Act 2018
- Information Management Toolkit for Schools (IRMS)
- Information Commissioner's Office (ICO) Guidance
- Ofsted School Inspection Handbook

- School Privacy Notices for pupils, parents and staff

This framework outlines our comprehensive approach to data protection and ensures that the school manages personal data in a lawful, fair, and transparent manner.