St. Paul's SNS
Data Protection Policy

Signed: A. Colly Principal

Signed: Rev. John Cole Chairperson of BoM

Date: 10/2/26

1. Introduction

St. Paul's SNS Drogheda ("the School") is committed to protecting the personal data of pupils, parents/guardians, staff, and all individuals who interact with the School.
This policy outlines how the School collects, uses, stores, and secures personal data in compliance with:

EU General Data Protection Regulation (GDPR)

Data Protection Acts 1988–2018 (Ireland)

Child Protection Procedures and relevant Department of Education guidelines

The School recognises the special importance of protecting children's data and applies the highest safeguarding standards.

2. Purpose

This policy aims to:

Promote transparency in how personal data is handled

Protect the rights and privacy of all data subjects

Ensure compliance with GDPR and national legislation

Provide clear procedures for data access, storage, sharing, and breaches

3. Scope

This policy applies to:

All pupils and parents/guardians

Teaching and non-teaching staff

Board of Management

Volunteers, contractors, and service providers

Anyone who has access to data controlled by St. Paul's SNS Drogheda

It covers all personal data held in:

Electronic systems

Paper files

Photographs and video recordings

CCTV

Communications platforms (email, apps, etc.)

4. Legal Basis for Processing

St. Paul's SNS Drogheda processes personal data under the following lawful bases:

- **Legal Obligation** – e.g., maintaining attendance records, child protection requirements
- **Public Interest / Official Authority** – delivery of primary education
- **Contract** – employment contracts for staff
- **Consent** – optional activities such as media use, school photographs, or extracurricular activities
- **Vital Interests** – emergencies relating to health or safety

5. Types of Data Collected

5.1 Pupil Data

- Name, address, date of birth
- PPS number (where required)
- Parent/guardian contact details
- Attendance records
- Academic records and assessments
- SEN data and support plans
- Behavioural notes
- Medical information (where necessary)
- Photographs/video (only with appropriate legal basis)

5.2 Staff Data

- Personal identifiers
- Employment and payroll details
- Garda Vetting information
- Training and performance records

5.3 Parent/Guardian Data

- Contact details
- Consent forms
- Communications with the School

6. Data Storage and Security

St. Paul's SNS Drogheda implements appropriate technical and organisational measures, including:

- Locked filing cabinets and restricted-access offices
- Password-protected IT systems and encrypted devices
- Access controls and user permissions
- Secure cloud services authorised by the Board of Management
- Regular updates, backups, and anti-virus protection
- Secure disposal via shredding or certified digital deletion
- Only authorised personnel have access to personal data on a strictly "need to know" basis.

7. Data Sharing

The School may share personal data with:

- The Department of Education
- Tusla and other child protection agencies
- HSE services (NEPS, Speech & Language, occupational therapy, etc.)
- Standardised testing providers
- School transport providers
- Approved third-party educational platforms

Data will only be shared where legally required or justified and never for commercial purposes. Where personal data is processed on behalf of the School by third-party service providers, St. Paul's SNS Drogheda ensures that appropriate Data Processing Agreements are in place, confirming that such processors comply with GDPR requirements and act only on the documented instructions of the School.

8. Photographs, Video & Media

St. Paul's SNS Drogheda will:

- Obtain consent where legally required
- Use photographs/videos only for the stated purpose
- Avoid identifying pupils by name in public material where possible
- Store media securely and delete it when no longer required

Consent may be withdrawn at any time.

9. CCTV

Where CCTV is used, it is for:

- Security and safety
- Protecting School property
- Supporting investigations of incidents

CCTV is not used in classrooms, toilets, or other sensitive areas.
Recordings are retained typically for 28 days, unless required for an investigation.

10. Data Retention

Retention follows the Department of Education Retention Schedule, including:

- Enrolment records: Permanent
- Accident/incident reports: 7 years
- Attendance records: 10 years
- CCTV footage: up to 28 days
- Staff records: 7 years after employment ends

Data is securely destroyed once retention periods expire.

11. Rights of Data Subjects

Individuals (or parents acting for their children) have the right to:

- Access their personal data
- Request rectification or erasure
- Restrict or object to processing
- Withdraw consent (where applicable)
- Data portability (rare in primary schools)
- Raise a data protection concern with the School in the first instance, in order to seek resolution
- Lodge a complaint with the Data Protection Commission

Requests will be responded to within one month. Requests for access to, or copies of, personal data must be made in writing to the School Principal. The School may request reasonable proof of identity before processing a request. Where a request is complex or numerous, the response period may be extended in line with GDPR requirements, and the requester will be informed accordingly. Requests may be refused or restricted where permitted by law, including where disclosure would adversely affect the rights of another individual or the welfare of a child.

12. Data Breach Procedure

A data breach includes loss, theft, unauthorised access, or accidental disclosure.
In the event of a breach, St. Paul's SNS Drogheda will:

1. Identify and contain the breach immediately
2. Assess the risk to affected individuals
3. Notify the Data Protection Commission within 72 hours, if required
4. Inform affected individuals where necessary
5. Document the incident and corrective measures

13. Roles and Responsibilities

- Board of Management – overall accountability for GDPR compliance
- Principal – day-to-day responsibility for data protection practices
- Data Protection Officer (if appointed) – advising, monitoring, handling access requests
- Staff – following data protection procedures and completing training

14. Policy Review

This policy will be reviewed:

- Bi-annually by the Board of Management
- As needed to reflect legislative or organisational changes