St. Columba's College Stranorlar

Data Protection Policy

March 2026

Contents

1. Introduction and Rationale

1.1 Mission Statement and Ethos

St. Columba's College is a Mercy Catholic Voluntary Secondary School within the CEIST Trust and is committed to **'The pursuit of excellence in a caring environment.'** Protecting the personal information of all members of the school community (students, staff, and parents) is essential to maintaining trust and respect within this environment.

1.2 Rationale and Legal Compliance

This policy outlines how St. Columba's College ensures compliance with data protection legislation, specifically the **EU General Data Protection Regulation (GDPR) 2016/679** and the **Data Protection Acts 1988–2018**. The College is committed to protecting the fundamental rights and freedoms of individuals, particularly their right to privacy and the protection of their personal data.

1.3 Scope and Application

This policy applies to all **Personal Data** and **Special Category Data** (as defined in Section 2.1) processed by the College, regardless of whether the data is held in physical (paper) or electronic form. The policy applies to:

- The Board of Management (BoM)
- All teaching and non-teaching staff (Permanent, Temporary, and Substitutes)
- All students and their parents/guardians
- Others, including prospective students/staff and contractors/volunteers

2. Definitions and Roles

2.1 Key Definitions

Term	Definition in the Context of the College
Personal Data	Any information relating to an identified or identifiable person (Data Subject). This includes names, addresses, photos, student numbers, assessment grades, and financial information.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning health (e.g., medical conditions, SEN needs) or sexual orientation. This data requires extra protection.
Processing	Any operation performed on personal data, such as collection, recording, storage, consultation, transmission, or erasure.
Data Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. **The Board of Management of St. Columba's College is the Data Controller.**
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.
Data Subject	The identified or identifiable natural person to whom the data relates (e.g., a student, a staff member, a parent).

2.2 Data Protection Roles and Responsibilities

- **Data Controller:** The **Board of Management (BoM)** of St. Columba's College holds the ultimate responsibility for data processing and compliance.
- **Data Protection Officer (DPO):** The DPO is formally appointed by the BoM to monitor internal compliance, advise the school, and act as the primary contact point with the Data Protection Commission (DPC) and data subjects.
- **Principal:** The Principal is responsible for the day-to-day implementation of the policy, ensuring all staff are aware of their responsibilities.
- **Staff:** All staff members are responsible for processing data in accordance with the policy and immediately reporting any actual or suspected data breaches to the Principal/DPO.

3. Core Data Protection Principles

The College adheres to the six core principles governing the processing of personal data:

3.1 Principle 1: Lawfulness, Fairness, and Transparency

Data is collected only where there is a lawful basis (e.g., legal obligation, performance of a contract, or explicit consent) and is processed fairly and transparently. Data Subjects are informed about how their data is used (via Privacy Notices).

3.2 Principle 2: Purpose Limitation

Data is collected only for specified, explicit, and legitimate purposes (e.g., education, welfare, administration) and is not processed in a manner that is incompatible with those purposes.

3.3 Principle 3: Data Minimisation and Accuracy

The data collected is adequate, relevant, and limited to what is necessary for the stated purpose. The College takes every reasonable step to ensure that personal data is accurate and, where necessary, kept up to date.

3.4 Principle 4: Storage Limitation

Data is 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, in line with the College's official Data Retention Schedule.

3.5 Principle 5: Integrity and Confidentiality (Security)

Personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, and against accidental loss, destruction, or damage, using appropriate technical or organizational measures. Data will be stored securely so that confidential information is protected.

3.6 Principle 6: Accountability

The Data Controller (BoM) is responsible for, and must be able to demonstrate compliance with, all the principles outlined above. All data processing activities are documented.

3.7 Lawful Basis for Processing

The College must identify a lawful basis under GDPR Article 6 for every data processing activity. The primary lawful bases relied upon are:

- **Legal Obligation:** Processing necessary for compliance with a legal obligation to which the College is subject (e.g., DES returns, Child Protection legislation, employment law).
- **Public Interest:** Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the College (i.e., operating a school, providing education).
- **Contract:** Processing necessary for the performance of a contract to which the data subject is party (e.g., staff employment contracts).
- **Legitimate Interests:** Processing necessary for the legitimate interests pursued by the College or a third party (e.g., CCTV operations, school security, fundraising), provided these interests are not overridden by the rights of the data subject.

Special Category Data: Processing data concerning health or other special categories of personal data (e.g., SEN needs, religious belief) requires an additional lawful condition under GDPR Article 9. The College relies on conditions such as substantial public interest and provision of health or social care.

4. Rights of the Data Subject

All Data Subjects (students, staff, parents) have specific rights regarding their personal data held by the College.

4.1 The Right of Access (SAR)

Data Subjects have the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data. Requests must be submitted in writing to the **Principal** and will be dealt with within the statutory timeframe (usually one calendar month).

4.2 Other Data Subject Rights

Data subjects (students, staff, and parents/guardians) also have the following rights:

- **Right to Rectification:** To have inaccurate data corrected or incomplete data completed without undue delay.
- **Right to Erasure ("Right to be Forgotten"):** To request the erasure of personal data where there is no compelling legal basis for its continued retention and processing.
- **Right to Restriction of Processing:** To restrict how their data is processed in certain circumstances, such as while accuracy is being verified.
- **Right to Data Portability:** To receive and transmit their personal data to another controller in a structured, commonly used, and machine-readable format (where processing is based on consent or contract).
- **Right to Object:** To object to processing based on grounds of public interest or the College's legitimate interests, unless the College demonstrates compelling legitimate grounds that override those interests.
- **Right not to be subject to automated decision making**: This right applies in specific circumstances (as set out in GDPR Article 22).
- **Right to Withdraw Consent:** In cases where St Columba's College is relying on consent to process your data, you have the right to withdraw this at any time, and if you exercise this right, we will stop the relevant processing.
- **Limitations on Rights**: While St Columba's College will always facilitate the exercise of your rights, it is recognised that they are not unconditional: St Columba's College may need to give consideration to other obligations.
- **Right to Complain**
    - If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Principal who is responsible for operational oversight of this policy.
    - A matter that is still unresolved may then be referred to St Columba's College's Data Controller (i.e., the Board of Management) by writing to the Chairperson c/o school.
    - Should you feel dissatisfied with how we have addressed a complaint or concern that you have raised, you have the right, as data subject, to bring the matter to the attention of the Irish Data Protection Commission.

5. Data Inventory and Retention

To ensure full compliance with the "Storage Limitation" principle, St. Columba's College maintains a detailed **Data Map** and **Record of Processing Activities (ROPA)**.

The definitive, granular schedule of all data categories, the specific legislative basis for their collection, and their mandated storage durations are maintained in the [St. Columba's College Data Retention Policy 2026].

This Data Protection Policy serves as the legal framework, while the Retention Policy acts as the technical index for the following record types:

- **Student Personal Data:** Including PPSN, Mother's Birth Name (for P-POD), identification photographs, medical information, and Irish language exemptions.
- **Academic & Behavioural Records:** Term reports, State Exam results, JCPA data, disciplinary files, and bullying investigation reports.
- **Welfare & SEN Records:** Psychological assessments, IEPs, Child Protection records (retained indefinitely), and Guidance (Therapeutic vs. Educational) notes.
- **Administrative & Governance:** Board of Management (BOM) Minutes (indefinite), Agendas, Attendance sheets, and Section 29 Appeal records.
- **Staff & Financial Records:** Personnel files, Garda Vetting outcomes, and Revenue/Payroll documentation.

6. Data Security & Breach Management

6.1 Physical and Digital Security

- **Physical Security:** Paper records are stored in locked, fire-resistant cabinets with restricted access.
- **Digital Security:** Use of encrypted school servers, role-based access in administrative software, and strong password protocols.

6.2 Device & Display Security

- **Hardware:** Laptops and desktops used for school business must be password/passcode protected and never left unattended while logged in.
- **Projection Screens:** Staff must ensure that no sensitive personal data (e.g., administrative software profiles, medical notes, or grades) is visible on projection screens in classrooms or common areas when students or unauthorised persons are present. Use of the "Freeze" or "Blank" screen function is mandatory when navigating between sensitive documents.

6.3 Breach Protocol & Reporting

- **Internal Reporting:** Any staff member who discovers or suspects a data breach (e.g., loss of a laptop, accidental sharing of an email list, or unauthorized access to a system) **must inform the Principal immediately**.
- **Statutory Reporting:** Any suspected data breach will be reported by the school to the Data Protection Commission (DPC) within 72 hours where required.

7. Policy Implementation

7.1 Relationship to Other Policies and Sanctions

This policy is the cornerstone of our compliance framework and must be read alongside the following:

- **Data Retention Policy:** Providing the extensive list of data categories and disposal timelines.
- **Admissions Policy:** Regarding the processing of applicant data and waiting lists.
- **CCTV Policy:** Regarding the specific retention and overwriting protocols for security footage.
- **Anti-Bullying Policy & Code of Behaviour:** Regarding the creation and retention of disciplinary and investigation records.
- **Acceptable Use Policy (AUP) & AI Policy:** Regarding the digital footprint and data generated through school systems and artificial intelligence tools.
- **Child Protection Policy:** Regarding the permanent retention of safeguarding records.

7.2 Data Processors and Data Sharing

The College will, at times, share data with third-party Data Controllers (e.g., Department of Education and Skills, SEC, TUSLA) as required by legal obligations. When engaging third-party **Data Processors** (e.g., cloud-based systems, IT providers, software vendors) who process personal data on the College's behalf, the College will ensure:

- The processor provides **sufficient guarantees** regarding technical and organisational security measures.
- A formal, signed **Data Processing Agreement (DPA)** is always put in place to govern the processing activities and ensure compliance with GDPR.

7.3 Automated Processing and Artificial Intelligence (AI)

The College recognises that data processing may increasingly involve automated systems and Artificial Intelligence (AI) tools.

- **Principle Adherence:** All use of AI and automated data processing must fully adhere to the six core GDPR principles.
- **Automated Decision-Making (Article 22):** The College shall not use fully automated systems to make decisions that significantly affect a data subject (e.g., disciplinary action, assessment outcomes) without meaningful human review, in line with the data subject's **Right not to be subject to automated decision-making**.
- **DPIA for AI:** A **Data Protection Impact Assessment (DPIA)** is mandatory before implementing any new AI system or process that involves high-risk activities, such as large-scale profiling, monitoring, or biometric data processing of students or staff.
- **Security and Third-Party Tools:** Staff and students are **prohibited** from inputting personal data, sensitive school information, or confidential records into generic, third-party generative AI tools (e.g., ChatGPT, Gemini, etc.) unless a formal Data Processing Agreement (DPA) is in place with the vendor and approved by the Data Controller.

8. Third-Party Data Sharing

The school sharing of data is conducted strictly under legal obligation or with explicit consent. Our data mapping identifies the following key third-party recipients:

- **Statutory Bodies:** Department of Education (DES), Revenue Commissioners, TUSLA, NCSE, and the State Examinations Commission.

- **Financial & Administrative Partners:** Bank for school accounts, and providers for staff deductions (Trade Unions, VHI/Laya, AVC providers).
- **Systems Providers:** Cloud-based management systems and the Department's **P-POD** system.

9. Ratification and Review

9.1 Implementation of Policy

St. Columba's College Data Protection Policy has been ratified by the Board of Management and formally adopted on **12th March 2026**.

We commit to ensuring its implementation in a manner that upholds the College's Catholic identity while fully respecting the rights and dignity of every student.

Signature: P. J. Mc Gowan **Date:** 12/3/26

(Chairperson, Board of Management)

Signature: _____ **Date:** 12/03/2026

(Principal)

9.2 Review of Policy

The school will monitor / review on a regular basis, and evaluate the policy and all related work and procedures to ensure legal compliance and the maintenance of best practices.

Date for Review: March 2028

Appendix 1: Reference Sites and Resources

This list is provided for staff and parents/guardians to access reliable, official information on Data Protection and GDPR.

Reference	URL
Data Protection Act 2018	http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
General Data Protection Regulation (GDPR official text) 2016	https://eur-lex.europa.eu/eli/reg/2016/679/oj
General Data Protection Regulation (GDPR unofficial web version) 2016	https://gdpr-info.eu/
GDPR for Schools website	https://gdpr4schools.ie/
Data Protection for Schools	http://dataprotectionschools.ie/en/
Irish Data Protection Commission (DPC)	https://www.dataprotection.ie/
Data Breach Report (DPC link)	https://forms.dataprotection.ie/report-a-breach-of-personal-data
European Data Protection Board (EDPB)	https://edpb.europa.eu/
EDPB Guidelines, Recommendations and Best Practices on GDPR	https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
DES Data Protection Page	https://www.education.ie/en/The-Department/Data-Protection/Information.html
PDST Technology in Education	https://www.pdsttechnologyineducation.ie
Cyber Security Centre (Ireland)	https://www.ncsc.gov.ie/