



DATA MANAGEMENT & POPIA COMPLIANCE POLICY (2026)

1. DOCUMENT CONTROL

Policy Owner	SMT and Board of Governors
Drafted By	SMT
Date of Approval	01 March 2026
Review Date	January 2027
Related Policies	Staff Code of Conduct & Disciplinary Policy (2026); Admissions Policy (2026); Social Media & Digital Citizenship Policy (2026); Financial Stewardship & Procurement Policy (2026); Substance Abuse Policy (2026).

2. PREAMBLE & ETHOS ALIGNMENT

At Loreto Convent School, we believe that every person is created with inherent dignity. Respecting a person's privacy is an extension of respecting their dignity.

Guided by the charism of **Mary Ward**, this policy is anchored in:

- **Sincerity:** We are transparent about *why* we collect data and *how* we use it. We do not use data for hidden agendas (e.g., selling lists to marketers).
- **Justice:** We protect the vulnerable. The data of a child is entitled to special protection under South African law.
- **Truth:** Our data practices are what we say they are. We do not collect data for one stated purpose and use it for another. Transparency is not merely a legal obligation — it is a moral one.
- **Freedom:** Individuals cannot be truly free when their personal information is held carelessly, shared without consent, or used against them. We protect data because we protect freedom.
- **Accompaniment:** When a learner or family member comes to us with a concern about their data — to access it, correct it, or ask that it be removed — we walk alongside them. We do not treat data subject rights as an inconvenience; we treat them as an expression of the dignity we are called to uphold.

In our Catholic tradition, the protection of the vulnerable is not a regulatory matter — it is a moral imperative. The data of children, families in financial hardship, and learners with learning barriers or medical conditions deserves not only legal protection but pastoral care in how it is held, shared, and used.

3. LEGISLATIVE CONTEXT

This policy is drafted in compliance with:

- *Constitution of the Republic of South Africa, 1996 — Section 14 (Right to Privacy) and Section 32 (Right of Access to Information). POPIA and PAIA give legislative effect to these constitutional rights.*
- *Information Regulator (South Africa) — guidance notes and regulations issued under POPIA.*
- *Protection of Personal Information Act (POPIA), 4 of 2013.*
- *Promotion of Access to Information Act (PAIA), 2 of 2000.*
- *General Data Protection Regulation (GDPR) (where applicable to foreign parents).*

4. DEFINITIONS

Data Subject: The person to whom the data relates (Learner, Parent, Staff, Alumni).

Personal Information: Any data that identifies a person (ID number, photo, address, religion, medical history).

Operator: A third-party provider who processes data for us (e.g., d6 Communicator, Cloud Storage Provider, Payroll Firm).

Processing: Collecting, recording, storing, sharing, or destroying data.

Responsible Party: The School (Loreto Convent School).

5. ROLES AND RESPONSIBILITIES

5.1. The Information Officer (IO)

Role: The Executive Principal is the statutory IO.

Duties: Ultimate accountability for data breaches, PAIA manual updates, and POPIA compliance.

5.2. The Deputy Information Officer (DIO)

Role: The School Bursar or IT Manager.

Duties: Daily management of data security, staff training, and responding to “Access to Information” requests.

5.3. All Staff

Duty: To treat learner and parent data as confidential. A breach of this policy is a disciplinary offence.

6. CONDITIONS FOR LAWFUL PROCESSING

6.1. Accountability

The School takes full responsibility for data it holds. We do not blame “the system” for leaks.

6.2. Processing Limitation (Minimality)

- We only collect data that is **absolutely necessary**.
- *Example: We need a parent’s ID for debt collection (Contract), but we do not need to know their political affiliation.*

6.3. Purpose Specification

- Data is collected for: Educational administration, communicating with parents, medical emergencies, and statutory reporting (GDE/SASAMS).
- Data will **never** be sold or given to commercial third parties without consent.

6.4. Security Safeguards

- **Physical Files:** Learner profiles are kept in a lockable fire-proof filing room. Keys are restricted to Admin Staff.
- **Digital Files:** All school laptops must be password-protected. The server is protected by a firewall and anti-virus software.
- **Clean Desk Policy:** Teachers may not leave mark sheets or learner profiles lying open on desks in empty classrooms.

6.5. Further Processing Limitation

Personal information collected for one purpose will not be processed for an unrelated or incompatible purpose without the data subject’s consent. For example, a parent’s contact details collected for communication about their child may not be used for fundraising campaigns without a separate consent.

6.6. Information Quality

The school takes reasonable steps to ensure that personal information held is complete, accurate, not misleading, and updated where necessary. Parents and staff are encouraged to notify the school of changes to their personal information.

6.7. Openness

The school maintains a PAIA Manual (publicly available on request) that describes the categories of personal information held, the purposes for which it is held, and the process for accessing or correcting it. The Information Officer is responsible for keeping this manual current.

6.8. Data Subject Participation (see also Section 10 below)

Data subjects have the right to access their own information, request corrections, and in certain circumstances object to processing. Refer to Section 10 for the full procedure.

7. SPECIAL DATA RULES

7.1. Photos and Social Media

- **Consent:** Parents sign a “Media Consent” form at admission.
- **Opt-Out:** Parents have the right to revoke this consent. A list of “No-Photo” learners is maintained by the Marketing Office.
- **Tagging:** The school will never “tag” a learner’s personal profile in photos on public platforms (Facebook/Instagram).

7.2. WhatsApp & Telegram Groups

- **Official Channels:** WhatsApp groups are for logistics only (e.g., “Bus is late”).
- **Prohibition:** Staff may **not** post:
 - Learner marks/results.
 - Photos of learners (unless it is a closed, secure group).
 - Details of a child’s medical condition or disciplinary issues.

7.3. Medical Information

- Details of allergies, HIV status, or psychological conditions are **Special Personal Information**.
- This data is restricted to the School Nurse, Principal, and the specific Class Teacher who needs to know for safety. It is *not* shared in the general staff room.

8. OPERATOR AGREEMENTS (THIRD-PARTY PROCESSORS)

1. The school uses third-party operators to process personal information on its behalf, including but not limited to: d6 Communicator (parent communication), SASAMS (learner records), cloud storage providers, and the payroll processing firm.
2. In terms of Section 21 of POPIA, operators may only process personal information with the knowledge and authorisation of the school, and must treat such information as confidential.
3. Before engaging any new operator that will process personal information, the school must:
 1. satisfy itself that the operator has adequate data protection measures in place;
 2. conclude a written data processing agreement obliging the operator to comply with POPIA and to notify the school immediately of any data breach; and
 3. record the operator in the school’s Operator Register (maintained by the DIO).
4. The DIO is responsible for reviewing all operator agreements annually.

9. DATA BREACH PROTOCOL

In the event of a breach (e.g., a teacher loses a USB stick with mark sheets, or the server is hacked):

1. **Report:** The staff member must report it to the IO immediately (within 1 hour).
2. **Contain:** IT locks down the affected accounts.
3. **Notify:** The IO must notify the **Information Regulator (South Africa)** and the affected Data Subjects (Parents) as per Section 22 of POPIA.
4. **Mitigate:** The school must explain what steps are being taken to fix the issue.

10. DATA SUBJECT RIGHTS

- 10.1 In terms of POPIA, every data subject (learner, parent, staff member, or alumni) has the right to:
- a) be notified that their personal information is being collected and the purpose for which it is used;
 - b) access the personal information the school holds about them;
 - c) request correction or deletion of inaccurate, irrelevant, or out-of-date information;
 - d) object, on reasonable grounds, to the processing of their personal information; and
 - e) submit a complaint to the Information Regulator if they believe their rights have been infringed.
- 10.2 Requests to exercise any of these rights must be submitted in writing to the Information Officer (Executive Principal) or the Deputy Information Officer.
- 10.3 The school will acknowledge the request within five (5) school days and respond substantively within 21 days, or such extended period as POPIA permits.
- 10.4 The school will not charge a fee for reasonable access requests. A fee may be charged for manifestly excessive or repetitive requests, in line with the PAIA fee schedule.

11. STAFF AWARENESS AND TRAINING

- 11.1 All staff who process personal information as part of their role must receive basic POPIA awareness training. This training is coordinated by the DIO and takes place at the start of each academic year.
- 11.2 New staff members receive POPIA awareness as part of their induction.
- 11.3 A breach of this policy is a disciplinary offence under the Staff Code of Conduct & Disciplinary Policy (2026).

12. RETENTION & DESTRUCTION

- 1) **Learner Profiles:** Retained for **5 years** after the learner leaves (in case of reference requests).
- 2) **Financial Records:** Retained for **5 years** (SARS requirement).
- 3) **Destruction:** Paper files are shredded (not just thrown in the bin). Digital files are permanently deleted.
- 4) **Staff Records:** Retained for 5 years after employment ends (UIF, PAYE, and reference purposes).
- 5) **CCTV Footage:** Retained for a maximum of 90 days unless preserved as evidence in an ongoing disciplinary or legal matter.

The school's full PAIA Manual, which sets out the complete retention schedule for all categories of personal information, is available on request from the Information Officer.

13. APPROVAL

Signed on behalf of the Board of Governors:



01 March 2026

Date: _____

Fatima Rawjee

Chairperson: Board of Governors

Signed by the Executive Principal:



01 March 2026

Date: _____

Suzette Truter

Executive Principal