
Records Management, Retention & Disposal Policy

1. Policy Statement

The Guru Nanak Institute of Global Studies (GNI) is committed to the systematic, secure, and responsible management of institutional records throughout their lifecycle. This policy establishes a unified framework to ensure records are created, maintained, accessed, retained, and disposed of in a manner that supports academic accountability, institutional transparency, privacy protection, and operational continuity.

2. Purpose

The purpose of this policy is to:

- Establish consistent standards for records creation, storage, retention, and disposal;
- Protect personal, academic, financial, and institutional information;
- Ensure records are accessible, reliable, and auditable when required; and
- Support ethical, lawful, and efficient disposal of records at the end of their retention period.

3. Scope

This policy applies to:

- All physical and digital records created, received, or maintained by GNI in the course of academic and administrative operations;
- All faculty, staff, contractors, and students who create or handle institutional or student records; and
- Records related to governance, admissions, teaching and learning, research, finance, human resources, and information technology.

4. Definitions

- Record:** Any recorded information, regardless of format, created or received in the course of institutional activity.
- Retention Period:** The minimum length of time a record must be retained before eligible disposal.

- **Disposal:** Secure, documented destruction or anonymization of records once retention requirements are met.
- **Confidential Record:** A record containing personal, academic, financial, or proprietary information.
- **Archive:** Records preserved permanently due to legal, historical, academic, or institutional value.

5. Records Lifecycle Management

5.1 Creation and Classification

Records must be created using approved institutional systems or templates and classified according to their function (e.g., governance, academic, student, financial, human resources, research).

5.2 Storage and Access

Records are stored in **secure, access-controlled physical or digital repositories**. Access is restricted to authorized personnel based on role and operational need.

5.3 Retention

Records are retained in accordance with **approved retention schedules** that reflect operational, legal, academic, and accountability requirements. Retention schedules are reviewed periodically and maintained as institutional records.

5.4 Disposal

Once retention requirements are met, records are securely disposed of using methods appropriate to the record type (e.g., shredding, permanent digital deletion). All disposals must be documented.

Category	Examples	Minimum Retention	Responsible Office
Governance Records	Board minutes, bylaws, policies	Permanent	Office of the President
Academic Records	Course outlines, grades, transcripts, evaluations	Permanent	Registrar
Student Records	Admissions, attendance, disciplinary actions	7 years post-withdrawal or graduation	Registrar
Financial Records	Invoices, payroll, audit reports	7 years	Finance Office
Human Resources	Employment files, evaluations	7 years after termination	HR

Research Records	Ethics approvals, grant documentation	5 years post-project	Research Office
IT & Digital Logs	System access logs, backups	2 years	IT Services
Marketing & Communications	Campaign materials, media releases	3 years	Communications

(Detailed retention schedule provided in Appendix A – reviewed every 3 years.)

7. Roles and Responsibilities

Role	Responsibilities
Board of Governors	Approves the policy and ensures institutional compliance with DQAB/PTIRU standards.
President/CEO	Ensures enforcement, oversight, and resource allocation for record security.
Registrar	Maintains official student academic records and oversees retention timelines.
Chief Information Officer	Implements cybersecurity protocols, encryption, and access control systems.
Department Heads	Classify and manage departmental records; ensure secure disposal.
All Employees & Faculty	Adhere to this policy and participate in annual data protection training.

8. Security and Privacy

- Records containing personal or confidential information must be stored on **approved secure systems**.
- Institutional records may not be stored on personal devices or external platforms without authorization.
- Any suspected data breach must be reported immediately in accordance with the Privacy & Data Protection Policy.

9. Disposal and Audit Trail

All record disposal must be:

- Authorized by the responsible office;
- Documented in a **Record Disposal Log** (record type, date, method, authorization); and
- Available for internal or external audit review.

10. Training and Compliance

- Records management and privacy training is provided during onboarding and through periodic refreshers.

- b. Compliance audits may be conducted to ensure adherence to this policy.
- c. Non-compliance may result in corrective or disciplinary action in accordance with institutional policies.

11. Review and Continuous Improvement

This policy is reviewed **every three (3) years**, or earlier if required due to institutional or legislative change. Reviews are conducted through established quality assurance processes to ensure ongoing effectiveness and alignment with best practices.

12. Related Policies

- (ADM-026) Privacy & Data Protection Policy
- (ADM-004) Institutional Quality Assurance Policy
- (SP-012) Academic Integrity and Misconduct Policy
- (ADM-028) Copyright and Intellectual Property Policy
- (ADM-025) Faculty and Staff Codes of Conduct

Appendix A – Detailed Retention Schedule

(To be developed with departmental input and retained as a living document linked to the Institutional Quality Assurance System.)