



BENEDICT XVI CATHOLIC INTERNATIONAL INSTITUTE

of Higher Education

DATA PROTECTION POLICY

DATA PROTECTION POLICY

Document Control

Policy Title:	Data Protection Policy
Institution:	Benedict XVI Catholic International Institute of Higher Education (BCI Campus)
Policy Owner:	Quality Assurance Unit
Approved By:	Academic Board and Governing Council
Effective Date:	31/01/2026
Version:	1.0
Next Review Date:	
Related Documents:	• Sri Lanka Personal Data Protection Act, No. 9 of 2022. • Draft Directions on the Formation of the Data Protection Authority (ICTA, 2023). • University Grants Commission (UGC) Circulars on Student Information Management. • Student Disciplinary Procedure • Assessment Regulations
Contact:	

1 Overview

BCI Campus operates in a data-driven educational environment and recognises that all personal and institutional data entrusted to the Campus must be protected, secured, and managed responsibly.

BCI acknowledges that inappropriate data use may cause reputational, regulatory, financial, or operational damage to the institution, its students, staff, and partners. This policy establishes a framework ensuring the confidentiality, availability, and integrity of all personal data processed by BCI.

1.1 Purpose

The purpose of this policy is to:

- Ensure full compliance with the Personal Data Protection Act, No. 9 of 2022.
- Provide a consistent and secure approach to the collection, storage, use, sharing, and disposal of personal data.
- Protect the rights of students, staff, and all data subjects connected to BCI.
- Promote responsible data-management practices across all academic, administrative, and digital systems.
- Support BCI's operational, educational, and regulatory functions through accurate, reliable data.

1.2 Scope

This policy applies to all personal data processed by:

- Academic faculties and departments
- Registry & Examinations
- Finance Division
- HR & Recruitment
- IT Services and LMS
- Library and digital resource systems
- External service providers (cloud storage, LMS, payment gateways, etc.)

It covers:

- All staff (full-time, part-time, visiting, contract)
- All students (internal, external, postgraduate)
- Applicants
- Alumni
- Contractors
- Visitors and third-party service providers

1.3 Legal & Regulatory Framework

BCI's Data Protection Policy aligns with the following:

- Personal Data Protection Act, No. 9 of 2022 (Sri Lanka)
- Regulations and directions issued by the Data Protection Authority of Sri Lanka
- UGC Circulars on student data confidentiality and IT governance
- Ministry of Education guidelines on institutional data and digital learners
- International partner body requirements, including Chartered Management Institute (CMI) standards

2 Definitions

2.1 Personal Data

Information relating to an identified or identifiable individual (name, NIC, contact details, academic records, etc.).

2.2 Special Category Personal Data

Sensitive data requiring explicit consent (medical records, disability information, biometric data).

2.3 University Data

All data generated or held by BCI for academic, administrative, research, financial, or operational activities.

2.4 Data Subject

Any person whose data is processed by BCI.

2.5 Data Controller

BCI Campus, determining the purposes and means of processing personal data.

2.6 Data Processor

Any internal unit or external service provider processing data on behalf of BCI.

2.7 Data User

Staff or authorized individuals accessing data for legitimate institutional purposes.

3 Categories of Personal Data Collected

3.1 Personal Data

- NIC/Passport details
- Full name & date of birth
- Contact information
- Educational history
- Employment history (staff)
- Financial information for fees, sponsorships, scholarships

3.2 Special Category Data (processed only with explicit consent)

- Medical and health information
- Disability-related needs
- Emergency contacts

3.3 System-Generated Data

- LMS login records
- Attendance logs
- ICT infrastructure access trail

4 Principles of Data Processing

BCI follows the PDPA principles (Sections 5–13):

- Lawfulness, fairness, and transparency
- Purpose limitation – Used only for legitimate functions
- Data minimization – Only essential information collected
- Accuracy – Maintaining updated, correct data
- Storage limitation – Retain only as long as necessary
- Security – Appropriate technical and organizational security
- Accountability – BCI ensures and demonstrates compliance
- Rights of Data Subjects – Access, correction, deletion, objection

4.1 Lawful Bases for Processing

BCI processes personal data on the following bases:

- Consent of the data subject
- Contractual necessity (admissions, enrolment, examinations)
- Legal obligation (MOE, UGC, tax, regulatory)
- Public interest in higher education governance
- Legitimate educational and administrative interest

4.2 Data Sharing & Disclosure

Personal data may be shared with:

- Ministry of Education, Sri Lanka
- University Grants Commission (UGC)
- Sri Lanka Examinations Department
- Chartered Management Institute (CMI)
- Learning Management Systems (LMS) & digital platforms
- Cloud hosting services compliant with PDPA
- Verified service partners (e.g., plagiarism detection tools)

BCI will never:

- Sell personal data
- Share data for unauthorized marketing

All sharing must comply with PDPA and internal authorization procedures.

4.3 Data Storage & Security Measures

BCI ensures the following safeguards:

- Access-controlled and monitored servers
- Password-protected systems and LMS
- Role-based access (administrator, academic, student)
- Encrypted databases & secure cloud services
- Locked physical storage for paper files
- Multi-factor authentication for critical systems
- Annual IT security audits
- Mandatory breach reporting within 72 hours to the DPA and senior management

4.4 Data Retention Periods

Aligned with Sri Lankan higher-education norms and PDPA:

Data Type	Retention Period
Student academic records	7 years
Examination scripts	5 years
HR records	Employment period + 10 years
Finance records	As per IRD regulations
Admission records	5 years
LMS logs	2 years (or as technically required)

4.5 Rights of Students and Staff

Under PDPA, individuals have the right to:

- Access their personal data
- Request corrections
- Withdraw consent (where applicable)
- Request deletion (except when restricted legally)
- Restrict or object to processing
- Know the purpose and handling of their data

BCI must respond to requests within **21 working days**.

5 Governance Structure

5.1 Data Protection Committee (DPC)

Chaired by: **Rector / President of BCI** Members include:

- Heads of Faculties
- Registrar
- Bursar
- IT Director
- Librarian
- HR Manager
- Examination Division Representative

5.2 Functions:

- Oversee governance of personal data
- Approve data-processing procedures
- Monitor PDPA compliance
- Review breach notifications
- Update policy annually

5.3 Data Owners, Operators & Users

5.3.1 Data Owners

(Senior officers such as Registrar, Deans, Directors, Bursar) Responsible for data quality, accuracy, lawful use, and access control.

5.3.2 Data Operators

Staff processing data daily (Registry, HR, Finance, IT). Responsible for implementing policy, ensuring secure handling, and reporting risks.

5.3.3 Data Users

Lecturers, admin staff, examiners. Must use data only for legitimate institutional purposes and follow confidentiality rules.

6 Data Breach Management

A data breach includes unauthorized access, loss, destruction, or disclosure. BCI will:

- Investigate immediately
- Contain and secure the affected systems
- Notify the Data Protection Committee
- Report to the Sri Lanka Data Protection Authority within 72 hours
- Notify affected individuals when required
- Document all incidents

7 Review & Amendments

This policy will be reviewed:

- Every two years, or
- When there are changes to PDPA regulations, MOE/UGC guidelines, or institutional needs.

Updates require recommendations from the Quality Assurance Unit and approval from the Governing Council.

8 Promulgation & Implementation

- This policy will be published on the BCI Campus website.
- It will be circulated to all staff and students.
- Training will be provided for all staff handling personal data.
- The Data Protection Committee and IT Division will lead implementation.

9 References

- Sri Lanka Personal Data Protection Act, No. 9 of 2022 - <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>
- Draft Directions on Data Protection Authority formation (ICTA, 2023) - <https://www.dpa.gov.lk/>
- UGC Circulars on student information management - [https://www.ugc.ac.lk/attachments/1130_IT%20Governance%20and%20management%20\(IT%20Policy\).pdf](https://www.ugc.ac.lk/attachments/1130_IT%20Governance%20and%20management%20(IT%20Policy).pdf)

---- End ----