GLOBTER INTERNATIONAL COLLEGE

DATA PROTECTION POLICY

Policies and Procedures for the Collection, Use, Storage, Security, Retention, and Disclosure of Personal Data

This policy sets out the principles, responsibilities, controls, and procedures by which Globter International College protects personal data relating to students, staff, applicants, alumni, partners, and other data subjects. It supports lawful, fair, and transparent processing and promotes confidence in the College's administrative, academic, and digital systems.

Document Control	Details
Document Title	Data Protection Policy
Institution	Globter International College
Document Type	Policy and Procedures
Applies To	Students, staff, applicants, contractors, visitors, and third parties processing data on behalf of the College
Responsible Officer	Principal / Designated Data Protection Lead
Approval Authority	College Management
Review Cycle	Annual or earlier where required by law, operational need, or significant change in processing activities
Effective Date	Upon approval

1. Purpose

This policy establishes the framework for the responsible handling of personal data by the College. It ensures that personal information is collected and used only for legitimate institutional purposes and that appropriate measures are in place to protect confidentiality, integrity, and availability.

It also supports compliance with applicable data protection requirements and provides a clear basis for accountability, oversight, and good administrative practice across the student life cycle and staff life cycle.

2. Scope

This policy applies to all personal data processed by the College in paper, verbal, electronic, audio-visual, and online form, whether held on College premises, on College systems, or by approved service providers.

It covers personal data relating to admissions, enrolment, teaching and learning, assessment, finance, human resources, library services, student support, alumni relations, marketing communications, complaints, disciplinary matters, and any other administrative or academic function.

3. Data Protection Principles

- Personal data shall be processed lawfully, fairly, and transparently.
- Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be used in a manner incompatible with those purposes.
- Personal data shall be adequate, relevant, and limited to what is necessary for the purpose for which it is processed.
- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data shall not be kept longer than necessary and shall be retained in line with approved retention arrangements.
- Personal data shall be protected by appropriate technical and organisational security measures.
- The College shall be able to demonstrate compliance through records, procedures, training, monitoring, and review.

4. Categories of Data Processed

The College may process identifying and contact information, admissions and enrolment records, academic records, attendance data, assessment results, financial information, welfare and support records, disciplinary records, IT usage logs, and other information reasonably necessary for institutional operations.

Where special category or otherwise sensitive information is processed, the College shall apply enhanced controls, need-to-know access, and appropriate lawful justification.

5. Lawful and Fair Processing

The College shall process personal data only where there is a lawful institutional basis to do so, such as fulfilling contractual and educational responsibilities, complying with legal obligations, protecting vital interests, performing tasks in the public or legitimate institutional interest, or obtaining valid consent where required.

Privacy information shall be communicated in a clear and accessible manner so that data subjects understand what information is collected, why it is collected, how it is used, how long it is retained, and with whom it may be shared.

6. Responsibilities

The following roles hold primary responsibilities for the implementation of this policy:

Role	Key Responsibilities
College Management	Approve the policy framework, allocate suitable resources, support oversight, and promote a culture of lawful and responsible data handling.
Principal / Designated Data Protection Lead	Oversee implementation of the policy, advise on compliance, coordinate incident response, support awareness, and monitor institutional practice.
Heads of Department	Ensure that personal data within their areas is processed only for legitimate purposes, access is controlled, records are managed appropriately, and staff follow procedures.
All Staff	Handle personal data confidentially, follow authorised procedures, complete required training, report breaches or concerns promptly, and avoid unauthorised disclosure.
Students	Use College systems responsibly, keep their own information accurate where required, and respect the confidentiality and privacy of others.
Third-Party Processors / Service Providers	Process College data only under approved arrangements, apply appropriate security controls, and comply with contractual and institutional requirements.

7. Collection and Use of Personal Data

Personal data shall be collected directly from the data subject wherever practical, or from authorised sources where collection from the individual is not feasible or not appropriate.

Departments shall collect only the information necessary for the stated purpose and shall avoid excessive, irrelevant, or duplicate collection.

Forms, portals, surveys, contracts, and digital systems used for collection shall include suitable notices or explanations where required.

8. Access, Confidentiality and Data Sharing

Access to personal data shall be restricted according to role, function, and legitimate need. Staff shall access only the information required for their duties.

Personal data shall not be disclosed to internal or external parties unless disclosure is authorised, lawful, proportionate, and necessary for a defined purpose.

Where third-party service providers process information on behalf of the College, suitable agreements and oversight arrangements shall be maintained.

9. Information Security Measures

The College shall maintain reasonable and proportionate measures to protect personal data from loss, unauthorised access, misuse, alteration, accidental destruction, or unlawful disclosure.

Security arrangements may include password controls, role-based access, encryption where appropriate, secure filing, restricted office access, backup, audit trails, secure disposal, and incident reporting procedures.

Users of College systems shall follow the College IT Policy and any relevant information security guidance.

10. Data Retention and Secure Disposal

Records containing personal data shall be retained only for as long as necessary to fulfil legal, academic, regulatory, administrative, or operational requirements.

Retention schedules shall be applied where available, and departments shall review records periodically to identify material for secure deletion, destruction, or archiving.

Paper records shall be shredded or otherwise disposed of securely. Electronic records shall be deleted or destroyed in a manner that reduces the risk of recovery.

11. Data Subject Rights and Requests

The College shall have procedures for responding, within a reasonable timeframe, to requests from individuals concerning their personal data, subject to legal limitations and institutional procedures.

Requests may relate to access, correction, updating, withdrawal of consent where applicable, restriction of certain uses, or other rights available under the relevant legal and institutional framework.

All such requests shall be directed promptly to the designated officer or office responsible for data protection and records management.

Procedure for Requests

1. Requests should be submitted in writing or through another accepted College channel.
2. The receiving office shall log the request and confirm receipt where appropriate.

3. Identity may be verified before personal data is released or amended.
4. The College shall review the request, consult relevant departments if necessary, and respond in line with applicable requirements.
5. Where a request cannot be fully met, the College shall explain the decision and any available next steps.

12. Data Breaches and Incident Management

Any actual, suspected, or attempted personal data breach shall be reported immediately to the designated officer, line manager, or other approved reporting point.

Reported incidents shall be assessed promptly to determine the nature of the breach, the data involved, the likely impact, immediate containment actions, notification requirements, and corrective measures.

The College shall document breaches and near misses, identify lessons learned, and implement remedial controls where required.

Breach Response Procedure

6. Contain the incident immediately wherever possible, including restricting access, recovering documents, or disabling compromised credentials.
7. Inform the designated officer without delay and record the time, nature, and circumstances of the incident.
8. Assess the categories of data involved, the number of affected individuals, and the likely risks or harms.
9. Take steps to mitigate impact, preserve evidence, and prevent recurrence.
10. Notify affected parties or relevant authorities where required by law or institutional decision.
11. Maintain a record of the incident, findings, actions taken, and follow-up measures.

13. Monitoring, Training and Awareness

The College shall promote awareness of data protection responsibilities through induction, policy communication, periodic guidance, and training relevant to role and risk.

Departments may be required to participate in audits, reviews, record checks, or compliance monitoring exercises relating to personal data handling.

Findings from monitoring shall be used to improve procedures, strengthen controls, and reduce institutional risk.

14. Non-Compliance

Failure to comply with this policy may result in corrective action, withdrawal of system access, disciplinary action, contractual remedies, or referral to the appropriate College authority, depending on the seriousness of the matter.

Deliberate misuse, reckless disclosure, or repeated failure to follow data protection requirements shall be treated as a serious matter.

15. Review of Policy

This policy shall be reviewed at least annually, or earlier where legal requirements, institutional processes, technology arrangements, or identified risks make revision necessary.

Updated versions shall be communicated through the College's approved document control and policy dissemination arrangements.

Appendix A: Examples of Personal Data Handled by the College

- Admissions applications, copies of qualifications, references, and interview notes.
- Student registration records, timetables, attendance, progression records, and award information.
- Assessment submissions, feedback records, academic integrity records, and appeal documentation.
- Payroll, recruitment, contract, leave, appraisal, and professional development information for staff.
- CCTV images, access logs, library borrowing records, system logs, and support service records where applicable.