GLOBTER INTERNATIONAL COLLEGE

IT POLICY

Policies and Procedures for Information Technology Management, Security and Acceptable Use

Document Control	Details
Document Title	IT Policy
Institution	Globter International College
Document Type	Policy and Procedures
Applies To	Students, academic staff, administrative staff, contractors and authorised users
Approved By	College Management
Review Cycle	Annual
Effective Date	Upon approval
Version	1.0

This policy sets out the principles, responsibilities, controls, and procedures that govern the use, management, security, and maintenance of information technology resources at Globter International College.

1. Purpose

The purpose of this policy is to ensure that the College's information technology resources are managed effectively, securely, and in a manner that supports teaching, learning, research, student administration, and institutional operations.

This policy promotes lawful, ethical, and responsible use of technology and establishes clear procedures for access, security, incident management, continuity, and monitoring.

2. Scope

This policy applies to all College-owned or College-managed information assets, including computers, laptops, mobile devices, servers, networks, wireless services, learning platforms, cloud systems, email accounts, software applications, digital records, audio-visual equipment, and online services.

It applies to all users who access College systems, whether on campus or remotely.

3. Policy Principles

- IT services shall support the academic mission, operational efficiency, and student experience of the College.
- Information systems shall be managed with due regard to confidentiality, integrity, availability, and data protection.
- Access to systems shall be granted on the basis of role, need, and authorisation.
- Users shall be accountable for their use of College technology and for safeguarding institutional information.
- The College shall maintain appropriate controls for cyber security, backup, disaster recovery, and service continuity.
- The College shall review its IT arrangements periodically to ensure suitability, legal compliance, and effectiveness.

4. Responsibilities

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

Role	Key Responsibilities
College Management	Approve the IT policy framework, allocate resources, oversee compliance, and support risk management.
IT Officer / IT Support Team	Maintain systems and networks, manage user accounts, implement security controls, provide support, and respond to incidents.
Heads of Department	Ensure that staff within their areas follow College procedures and report system risks or recurring issues.
Staff and Students	Use College systems responsibly, protect passwords and devices, complete required training, and report incidents promptly.
Data / Records Responsible Officers	Ensure digital records are handled, retained, and protected in accordance with College policies and legal requirements.

5. Acceptable Use of IT Resources

All users of College technology shall comply with the following acceptable use requirements:

- Use College systems for legitimate academic, administrative, and authorised institutional purposes.
- Access only the information, services, and applications for which the user has been authorised.
- Use respectful and lawful communication in email, messaging systems, online platforms, and digital learning environments.
- Not install unauthorised software, disable security features, or attempt to bypass access controls.
- Not use College systems for harassment, discrimination, fraud, copyright infringement, or any unlawful activity.
- Protect College devices from misuse, damage, theft, and unauthorised access.

6. Access Management Procedures

The College shall maintain formal procedures for user account creation, modification, suspension, and termination.

- Access requests shall be approved by the relevant authorised manager or designated officer.
- User accounts shall be issued according to the principle of least privilege and role-based access.
- Passwords shall be kept confidential and changed whenever compromise is suspected.
- Accounts of staff or students leaving the College shall be disabled or removed in a timely manner.
- Shared accounts shall be avoided unless operationally necessary and formally approved.

7. Information Security and Data Protection

The College shall take reasonable and proportionate steps to protect information and digital services.

- Anti-virus, endpoint protection, and security updates shall be maintained on managed devices.
- Sensitive information shall be stored only on authorised systems and shared only with authorised recipients.
- Portable devices and removable media shall be used with caution and, where possible, protected by encryption.
- Multi-factor authentication should be used for critical systems where available.
- Users shall not disclose passwords or security credentials to any other person.
- Personal data shall be collected, processed, retained, and disposed of in accordance with applicable legal and institutional requirements.

8. Learning Systems and Digital Services

The College may use digital platforms to support teaching, learning, assessment, communication, and student support services.

- Learning Management Systems and digital portals shall be maintained to support student access to course materials, notices, submissions, and feedback.
- Students shall be provided with appropriate information on how to access digital services, request assistance, and report technical issues.
- Where learning is delivered online or in blended mode, support channels such as email, helpdesk, recorded guidance, or live support sessions shall be made available as appropriate.
- System activity logs may be used for security, service improvement, and the investigation of suspected misuse, in accordance with law and College procedure.

9. Backup, Recovery and Business Continuity

Critical institutional systems and information shall be backed up at appropriate intervals, and reasonable arrangements shall be maintained for service restoration.

- Backup schedules shall be documented for key systems and records.
- Backup media and cloud backup services shall be protected against unauthorised access.
- Recovery procedures shall be tested periodically where feasible.
- Priority shall be given to restoring systems that support admissions, student records, teaching, finance, and core administration.

10. Software, Assets and Licensing

The College shall maintain proper control over hardware and software resources.

- Only licensed and approved software shall be installed on College-owned equipment.
- An inventory of major IT assets should be maintained and reviewed periodically.
- Procurement of IT systems shall consider compatibility, security, maintainability, data protection, and value for money.
- Obsolete or faulty equipment shall be disposed of securely and in accordance with data sanitisation requirements.

11. IT Support and Service Requests

The College shall maintain a procedure for logging and resolving IT issues.

- Users shall report hardware faults, software issues, access problems, and network interruptions through the designated reporting channel.
- IT support requests shall be logged, prioritised, and addressed according to urgency and operational impact.
- Support records may be reviewed to identify recurring issues, required upgrades, or training needs.

12. Incident Reporting and Response

Security incidents, suspected breaches, malware infections, phishing attempts, unauthorised access, data loss, or significant service outages shall be reported immediately to the designated IT contact or College management.

- The incident shall be logged and assessed for impact, urgency, and containment needs.
- Access may be restricted temporarily to protect systems or evidence during investigation.
- Where relevant, affected users or management shall be informed of service disruption or risk.
- Corrective and preventive measures shall be documented following incident closure.

13. Monitoring and Compliance

The College reserves the right, within the limits of law and institutional policy, to monitor the use of its IT resources for security, operational, and compliance purposes.

- Monitoring may include system logs, access histories, security alerts, storage usage, and network activity records.
- Any monitoring shall be proportionate, justified, and handled with appropriate confidentiality.
- Non-compliance with this policy may lead to corrective action, withdrawal of access rights, disciplinary procedures, or referral under other College policies.

14. Training and Awareness

The College shall promote good digital practice through orientation, guidance, and periodic awareness activities for staff and students.

- New staff and students should receive basic guidance on account use, password protection, and safe online conduct.
- Additional training may be provided on topics such as phishing awareness, data protection, secure records handling, and use of learning systems.

15. Review of the Policy

This policy shall be reviewed periodically, and normally on an annual basis, or earlier where changes in legal, technical, or operational requirements make revision necessary.

16. Related Documents

- Student Handbook
- Code of Conduct
- Admissions Policy and Procedures
- Assessment Policy
- Plagiarism Detection and Prevention Procedure
- Data protection and records management arrangements adopted by the College