Grand Asian University, Sialkot

Data Protection & Privacy Policy

(2025)

ALIGNED WITH UNITED NATIONS
Sustainable Development Goals 2030

SDG 16

PEACE, JUSTICE AND STRONG INSTITUTIONS

Promote peaceful and inclusive societies for sustainable development, provide access to justice for all

Document Reference
GAUS/Reg/DPP/2025

Version
Version 1.0

Approved on
2025

Review Cycle
Annual

TABLE OF CONTENTS

DATA PROTECTION & PRIVACY POLICY

The Data Protection and Privacy Policy shall come into force with immediate effect for all programmes of the Grand Asian University Sialkot (GAUS) and shall be applicable to all faculty members, staff, students, and associated third parties.

1.1 PURPOSE

To safeguard all personal, academic, and administrative data held by Grand Asian University Sialkot (GAUS), in compliance with the Prevention of Electronic Crimes Act (PECA) 2016, the pending Pakistan Data Protection Act and HEC Digital Guidelines. GAUS is committed to ensuring that data is collected, stored, processed, and disposed of responsibly and lawfully.

1.2 SCOPE

This Policy covers all digital and physical records of students, staff, applicants, alumni, and partners processed by GAUS systems and applies to:

i. All full-time, part-time, visiting, and contractual faculty members;
ii. All administrative, support, and technical staff;
iii. Students enrolled in any degree, diploma, or certificate programme;
iv. All third parties processing data on behalf of GAUS, including vendors and IT service providers;
v. All university-owned and personally-owned devices used to access GAUS data.

1.3 DEFINITIONS

For the purposes of this Policy, the following definitions shall apply:

i. "Personal Data" means any information relating to an identified or identifiable natural person, including name, contact details, academic records, financial information, and biometric data.
ii. "Data Controller" means the individual or office responsible for determining the purposes and means of processing personal data.
iii. "Data Processor" means any individual or third party that processes data on behalf of the Data Controller.
iv. "Data Subject" means the individual to whom personal data relates.
v. "Processing" means any operation performed on personal data, including collection, storage, use, disclosure, and deletion.
vi. "Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

1.4 KEY POLICY STATEMENTS

The following key statements shall govern the collection, use, and protection of data at GAUS:

Lawful Collection & Consent:

i. Only data that is necessary for a specific, stated purpose shall be collected.
ii. Explicit written consent shall be required for the use of photographs, testimonials, or sensitive personal information.
iii. Data pertaining to minors requires the written consent of a parent or legal guardian.

iv. Consent checkboxes shall be added to all existing admission and employment forms.

Access & Security:

v. Access to personal data shall be granted on a role-based, need-to-know basis only.

vi. Shared or generic accounts for accessing personal data are strictly prohibited.

vii. All physical records containing personal data shall be stored in locked cabinets with access logs maintained.

viii. Two-factor authentication (2FA) shall be enabled on all university email accounts.

Retention & Disposal:

ix. Student academic records shall be retained for a minimum of ten (10) years post-graduation.

x. Outdated or redundant data shall be securely disposed of by physical shredding or certified digital wiping.

xi. A simple data inventory spreadsheet shall be maintained by each administrative office.

Data Breach Response:

xii. Any suspected or confirmed data breach must be reported to the IT Office and Legal Office within 24 hours of discovery.

xiii. Affected individuals shall be notified promptly if the breach poses a risk of harm.

xiv. A post-incident review shall be conducted following every confirmed breach, and corrective measures implemented.

1.5 ROLES & RESPONSIBILITIES

i. Data Protection Focal Person (IT/Registrar's Office): Oversee policy compliance, coordinate audits, manage breach response, and maintain the data register.

ii. IT Office: Implement technical security controls, manage backups and encryption, conduct password hygiene training, and enforce access controls.

iii. HR, Admissions, and Examinations Offices: Handle data in accordance with this Policy, obtain required consents, and report any data anomalies to the IT Office.

iv. Legal Office: Advise on PECA 2016 compliance, manage external notifications in the event of a breach, and maintain records of consent and disclosure.

v. All Staff & Faculty: Protect assigned credentials, report suspicious data activity promptly, and complete annual data hygiene training.

vi. Vice Chancellor: Provide institutional leadership on data protection and approve all significant data-sharing agreements.

1.6 CONDUCT PROCEDURE

The following procedure shall be observed upon detection or reporting of a suspected violation:

Reporting:

i. Any member of the GAUS community may report a suspected violation to the IT Office or Registrar's Office or via the anonymous physical drop-box maintained by the Registrar's Office.

ii. Reports shall be acknowledged within 48 working hours and assigned a case reference number by the Registrar's Office.

Investigation:

iii. Upon receipt of a complaint, the relevant Committee shall convene within ten (10) working days.

iv. The Committee shall have authority to interview relevant parties and access all documentation pertaining to the case.

v. The Committee shall be permissible to conduct one or more than one session to investigate and probe the matter.

vi. Investigations shall be completed within thirty (30) working days from the first sitting; extensions may be granted by the Vice Chancellor.

vii. The quorum for a meeting of the Committee shall be a minimum of three members.

viii. In the event all members disagree among themselves, the case shall be referred to the Vice Chancellor for decision.

Decision & Notification:

ix. The recommendations and report of the Committee shall be submitted to the Vice Chancellor, who shall have power to accept, reject, or modify the recommendations.

x. The final notification of each case shall be published by the Registrar's Office and communicated to all concerned parties.

1.7 RIGHT OF APPEAL

The affected party shall have the right to submit an appeal against the first decision to the Appellant Committee within fifteen (15) days of publication of notification, failing which the first decision shall be considered as the final decision.

1.8 IMPOSITION OF PENALTIES

The following penalties may be imposed regarding data protection violations, singly or in combination:

i. Formal written warning recorded in the personal file;

ii. Mandatory data protection remedial training;

iii. Revocation of data access privileges;

iv. Suspension from duties for a defined period;

v. Termination of employment or expulsion from the University;

vi. Referral to FIA Cyber Crime Wing or other competent authority for criminal proceedings under PECA 2016;

vii. Any other penalty as deemed appropriate by the Vice Chancellor in light of the circumstances of the case.

1.9 MONITORING & COMPLIANCE

i. An annual self-assessment checklist shall be completed by each administrative office and submitted to the Data Protection Focal Person.

ii. A biannual password and access review shall be conducted by the IT Office.

iii. The Registrar's Office shall maintain a centralized register of all reported cases, breaches, outcomes, and pending matters.

iv. A quarterly compliance report shall be submitted to the Vice Chancellor.

v. Non-compliance with this Policy shall be addressed through the GAUS disciplinary process.

1.10 IMPLEMENTATION

i. A 30-minute data hygiene orientation module shall be incorporated into the existing staff and student induction programme via the LMS.

ii. Free password management tools and two-factor authentication shall be enabled on all university email accounts as a baseline security measure.

iii. Consent checkboxes and data handling clauses shall be added to all existing admission, employment, and partnership forms at zero additional cost.

iv. A simple data inventory spreadsheet shall be established and maintained by each office to track categories and locations of personal data held.

1.11 REVIEW & AMENDMENT

i. This Policy shall be reviewed annually by the the Registrar's Office, IT Office, and Legal Office.

ii. All amendments shall be aligned with current HEC guidelines and applicable national legislation.

iii. Proposed amendments shall be submitted to the Vice Chancellor for approval before coming into effect.

iv. The revised Policy shall be communicated to all stakeholders and updated on the GAUS official website within fifteen (15) days of approval.

Prepared By: Registrar's Office, GAUS

Signature: _____

Date: 19/11/25

Approved By: Vice Chancellor, GAUS

Signature: _____

Date: _____