Grand Asian University, Sialkot

ICT & Digital Technology Policy

(2025)

ALIGNED WITH UNITED NATIONS
Sustainable Development Goals 2030

SDG 4

QUALITY EDUCATION

Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all

Document Reference	Version
GAUS/Reg/ICT/2025	Version 1.0
Approved on	Review Cycle
2025	Annual

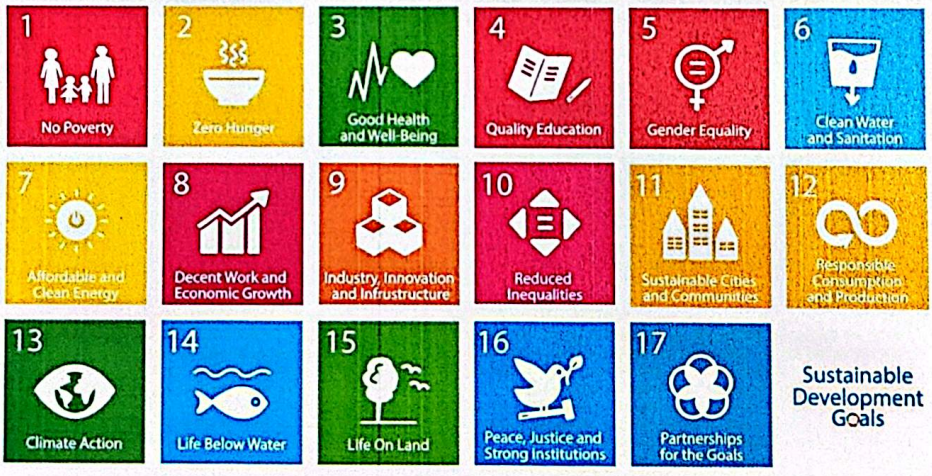

TABLE OF CONTENTS

ICT & DIGITAL TECHNOLOGY POLICY

The ICT and Digital Technology 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, and students.

1.1 PURPOSE

To ensure secure, efficient, and equitable use of GAUS's Information and Communication Technology (ICT) resources, supporting academic excellence while complying with the Prevention of Electronic Crimes Act (PECA) 2016.

1.2 SCOPE

This Policy applies to all university-owned devices, networks, cloud services, software, and third-party digital platforms accessed by any member of the GAUS community, including:

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. Third-party vendors and service providers granted access to GAUS ICT infrastructure;
v. All personally-owned devices used to access GAUS systems or networks (BYOD).

1.3 DEFINITIONS

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

i. "ICT Resources" means all university-owned or university-managed computing hardware, software, networks, telecommunications systems, data storage, and cloud platforms.
ii. "Acceptable Use" means the lawful, ethical, and purposeful use of ICT resources consistent with this Policy and GAUS values.
iii. "BYOD" (Bring Your Own Device) means the use of personally-owned electronic devices to access university networks, systems, or data.
iv. "Two-Factor Authentication (2FA)" means a security process requiring two distinct forms of verification before granting access to a system.
v. "Cyberbullying" means the use of digital platforms to intimidate, harass, threaten, or harm any member of the GAUS community.
vi. "Open Educational Resources (OER)" means educational materials that are freely available for use, adaptation, and redistribution.
vii. "PECA" means the Prevention of Electronic Crimes Act, 2016.

1.4 KEY POLICY STATEMENTS

The following key statements shall govern the use of ICT resources at GAUS:

Network & Security:

i. Access to university Wi-Fi requires valid institutional credentials; guest access shall be time-limited and logged.
ii. Only licensed or approved open-source software shall be installed on university-owned devices.

iii. Security patches and system updates shall be applied by the IT Office on a regular scheduled basis.

iv. Two-factor authentication (2FA) shall be mandatory on all university email and administrative system accounts.

Acceptable Use:

v. The following activities are strictly prohibited on university ICT resources: illegal downloads, access to gambling or pornographic content, incitement to hate speech, or any activity prohibited under PECA 2016.

vi. Personal use of ICT resources is permitted during designated breaks provided it is non-disruptive and does not consume excessive bandwidth.

vii. The use of Artificial Intelligence (AI) tools in academic work is permitted, subject to mandatory disclosure in the relevant submission.

viii. Users shall respect intellectual property rights and copyright law when accessing, sharing, or publishing digital content.

BYOD & Remote Access:

ix. Personally-owned devices used to access GAUS systems must have updated antivirus software and connect only via the secure university Wi-Fi or approved VPN.

x. Remote access to university systems shall require two-factor authentication.

xi. Lost or stolen devices with access to GAUS data must be reported to the IT Office immediately to enable remote wipe where applicable.

Digital Citizenship:

xii. All members of the GAUS community shall uphold institutional values in all online interactions and external digital representations.

xiii. Cyberbullying, sectarian content, defamatory statements, and partisan political activity are prohibited on university platforms.

xiv. Members shall cite digital sources properly and promote the use of Open Educational Resources (OER).

1.5 ROLES & RESPONSIBILITIES

i. **IT Office:** Maintain ICT infrastructure, enforce security controls, provide technical support, conduct digital awareness sessions, and review firewall logs on a weekly basis.

ii. **Department Heads:** Ensure all staff and students under their purview understand and comply with this Policy, and report any instances of misuse.

iii. **Faculty:** Model responsible and ethical technology use in all teaching and administrative activities, and integrate digital ethics into relevant coursework.

iv. **All Users:** Protect personal credentials, report suspicious digital activity to the IT Office immediately, and comply with all acceptable use requirements.

v. **Administration Office:** Advise on PECA 2016 compliance, review content monitoring requests, and manage any referrals to the FIA Cyber Crime Wing.

vi. **Vice Chancellor:** Provide institutional leadership on ICT governance, approve significant ICT policy changes, and ensure alignment with HEC digital directives.

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 ICT policy violations, singly or in combination:

i. Formal written warning recorded in the personal file;

ii. Mandatory digital ethics remedial training;

iii. Temporary or permanent revocation of ICT access privileges;

iv. Suspension from duties or academic activities 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. The IT Office shall conduct a quarterly security checklist review covering network integrity, access controls, and device compliance.

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 ICT policy violations, singly or in combination:

i. Formal written warning recorded in the personal file;

ii. Mandatory digital ethics remedial training;

iii. Temporary or permanent revocation of ICT access privileges;

iv. Suspension from duties or academic activities 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. The IT Office shall conduct a quarterly security checklist review covering network integrity, access controls, and device compliance.

ii. An annual user experience and compliance survey shall be embedded in existing student and staff feedback forms.

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

iv. Firewall logs shall be reviewed weekly by the IT Office; findings shall be reported to the Vice Chancellor on a quarterly basis.

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

1.10 IMPLEMENTATION

i. Digital etiquette posters shall be displayed in all computer laboratories and ICT areas; a policy summary shall be included in the LMS welcome module.

ii. Free Microsoft and Google digital literacy modules and a peer 'Tech Buddy' programme shall be established for ongoing user support.

iii. Free cloud backup solutions and built-in device encryption tools shall be used as primary data protection measures at zero additional cost.

iv. IT governance awareness shall be incorporated into the existing staff and student induction programme.

1.11 REVIEW & AMENDMENT

i. This Policy shall be reviewed annually by the IT Governance Committee and Registrar's 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: _____