SAI UNIVERSITY
CHENNAI

IT Policy

Use of Information and Communication Technology Resources

(2025 EDITION)

INDEX

1. Short Title and Commencement

1.1 This document shall be cited as the "SAI University – Chennai, Information Technology (IT) Policy", also referred to as the "Use of Information and Communication Technology Resources Policy."

1.2 This policy shall come into effect from the date of its approval by the competent authority of SAI University and shall remain in force until it is amended or replaced by a subsequent version.

1.3 All members of the University community, including faculty, staff, students, and authorized users, are required to adhere to this policy from the effective date of implementation.

2. Purpose

2.1 The purpose of this policy is to establish a comprehensive framework governing the responsible, ethical, and secure use of SAI University's Information and Communication Technology (ICT) resources.

2.2 This policy aims to:

- Ensure that all IT resources are used in alignment with the academic, research, administrative, and outreach objectives of SAI University.
- Promote integrity, confidentiality, and availability of information and technological systems.
- Safeguard the University's digital infrastructure from unauthorized access, misuse, or damage.
- Encourage the responsible and professional use of digital platforms and online communication tools.
- Ensure compliance with all applicable laws, regulations, and institutional policies related to information security, privacy, and intellectual property.

2.3 This policy serves as a guiding document for all members of the University community to uphold academic excellence, digital responsibility, and institutional integrity in the use of information technology.

3. Scope

3.1 This policy applies to all members of the SAI University community, including but not limited to:

- Faculty, administrative staff, and research personnel.
- Students, interns, and research scholars.
- Visiting faculty, consultants, and contractual employees.
- Vendors, contractors, and external partners who are granted access to University IT resources.
- Guests and authorized visitors who use temporary or limited network access provided by the University.

3.2 The policy governs the use, management, and protection of all Information Technology (IT) and Communication resources owned, leased, operated, or managed by SAI University, including but not limited to:

- Computers, servers, storage devices, and related hardware.
- Software applications, licensed tools, and databases.
- Network infrastructure, internet connectivity, and wireless services.

- Email systems, official communication platforms, and collaboration tools.
- University websites, portals, and digital learning environments.

3.3 This policy is applicable both on and off campus when accessing University systems remotely through authorized means such as VPNs, cloud services, or online portals.

3.4 All users are expected to comply with this policy to ensure the security, efficiency, and ethical use of the University's information and communication technology ecosystem.

4. Acceptable Use of IT Resources

4.1 General Principles

4.1.1 SAI University provides Information Technology (IT) and Communication resources to support its core missions of teaching, learning, research, innovation, and administration.

4.1.2 All users are expected to use these resources in a responsible, ethical, secure, and lawful manner, consistent with the values and reputation of the University.

4.1.3 The use of University IT resources is a privilege granted to members of the University community and may be revoked or restricted in cases of misuse or violation of this policy.

4.2 Institutional Use

4.2.1 University IT resources shall be used primarily for institutional purposes, including academic instruction, scholarly research, official communication, and authorized administrative functions.

4.2.2 All equipment, software, email systems, networks, and data generated or maintained on university systems are the property of SAI University. Users are custodians of these resources and must ensure their integrity and appropriate use.

4.2.3 The use of IT resources must:

- Support the mission and objectives of the University.
- Comply with applicable laws, copyright and intellectual property rights, and University regulations.
- Maintain the privacy, confidentiality, and security of information handled through these systems.

4.3 Personal Use

4.3.1 Limited personal use of University IT resources is permitted, provided that such use:

- Does not interfere with work, academic, or research responsibilities.
- Does not consume excessive system resources or impact network performance.
- Does not conflict with the mission or policies of the University.
- Does not involve personal business, profit-making, or political campaigning.

4.3.2 Users must ensure that personal use reflects the University's ethical standards and does not compromise institutional data, network security, or system performance.

4.4 Shared Responsibility

4.4.1 All members of the University community share a collective responsibility to:

- Protect IT systems and data from unauthorized access, modification, or misuse.
- Report any suspicious activity, cyber threats, or policy violations to the IT Department.
- Cooperate with University authorities in maintaining a safe and secure digital environment.

4.4.2 Users are reminded that any use of IT resources that compromises the integrity, security, or reputation of SAI University will be treated as a serious policy violation.

5. Prohibited Use

5.1 The use of SAI University's Information Technology (IT) and Communication resources is

subject to the highest standards of integrity, legality, and responsibility. Any activity that is inconsistent with the academic and administrative objectives of the University, or that violates laws, regulations, or institutional policies, is strictly prohibited.

5.2 Misuse of IT Resources

Users shall not use University IT resources to:

- Access, create, transmit, or store fraudulent, obscene, pornographic, threatening, defamatory, or harassing material.
- Engage in hate speech, cyberbullying, or discriminatory communication against individuals or groups.
- Disseminate false, misleading, or confidential information without authorization.
- Attempt to hack, breach, or circumvent any system or network security controls.
- Intentionally introduce viruses, malware, or malicious code into university systems or networks.
- Participate in unauthorized data mining, spamming, or phishing activities.
- Engage in activities that disrupt network performance, consume excessive bandwidth, or affect the accessibility of IT services for others.

5.3 Unauthorized Access and Use

The following actions are explicitly prohibited:

- Accessing or attempting to access accounts, systems, files, or data belonging to other individuals or departments without permission.
- Sharing user IDs, passwords, or authentication tokens with others.
- Using another person's credentials or identity for any purpose.
- Accessing University systems after termination of employment, enrollment, or association with the institution.
- Using personal devices or external storage on university networks without prior authorization from the IT Department.

5.4 Violation of Copyrights and Intellectual Property Rights

Users must not:

- Copy, download, distribute, or modify copyrighted materials or licensed software without appropriate permission.
- Use University systems to engage in illegal file-sharing, torrenting, or software piracy.
- Violate any terms of software licensing or contractual agreements made by the University.
- Use intellectual property belonging to the University, faculty, or students without acknowledgment or consent.

5.5 Unauthorized Commercial and Political Activities

University IT resources shall not be used for:

- Conducting personal business, commercial advertising, or promotional campaigns.
- Soliciting funds or services for private enterprises.
- Participating in or promoting partisan political campaigns or lobbying, except as legally permitted and institutionally approved.

5.6 Other Prohibited Activities

Users must not:

- Use IT resources to impersonate others, falsify information, or misrepresent identity.
- Disclose confidential or restricted data to unauthorized persons.
- Bypass security mechanisms such as firewalls, encryption systems, or access controls.
- Connect unapproved wireless access points or network devices to the University's infrastructure.
- Engage in any behaviour that damages the University's reputation or violates its code of conduct.

5.7 Compliance

Violations of this section will be treated as serious misconduct and may result in disciplinary action, including suspension of IT privileges, academic or administrative sanctions, or legal proceedings as deemed appropriate by the University authorities.

6. Prohibited Use

6.1 The use of SAI University's Information Technology (IT) and Communication resources shall adhere to the highest standards of integrity, legality, and responsibility. Any activity that is inconsistent with the academic or administrative objectives of the University, or that violates applicable laws, regulations, or institutional policies, is strictly prohibited.

6.2 Misuse of IT Resources

Users shall not use University IT resources to:

- Access, create, transmit, or store fraudulent, obscene, pornographic, threatening, defamatory, or harassing material.
- Engage in hate speech, cyberbullying, or discriminatory communication against any individual or group.
- Disseminate false, misleading, or confidential information without authorization.
- Attempt to hack, breach, or bypass any system, network, or data security controls.
- Intentionally introduce viruses, malware, or malicious code into university systems.
- Participate in unauthorized data mining, phishing, or spamming activities.
- Conduct actions that disrupt network performance or consume excessive bandwidth, affecting system availability for others.

6.3 Unauthorized Access and Use

The following activities are strictly prohibited:

- Accessing or attempting to access accounts, systems, or files belonging to others without explicit permission.
- Sharing user IDs, passwords, or authentication credentials with others.
- Using another person's login credentials or digital identity.
- Accessing University systems after termination of employment, enrollment, or association with the institution.
- Connecting personal devices or external storage to university networks without prior approval from the IT Department.

6.4 Violation of Copyrights and Intellectual Property Rights

Users must not:

- Copy, download, distribute, or modify copyrighted materials or licensed software without authorization.
- Use University systems for illegal file-sharing, torrenting, or software piracy.
- Violate software licensing agreements or intellectual property laws.
- Use University-owned intellectual property without acknowledgment or permission.

6.5 Unauthorized Commercial and Political Activities

University IT resources shall not be used for:

- Conducting private businesses, commercial advertising, or promotional campaigns.
- Soliciting funds or services for personal gain.
- Participating in or promoting partisan political activities, except as permitted by law and University policy.

6.6 Other Prohibited Activities

Users must not:

- Impersonate others, falsify information, or misrepresent identity.
- Disclose confidential or restricted data to unauthorized persons.
- Bypass security mechanisms such as firewalls, encryption, or authentication systems.
- Install or connect unauthorized network devices or wireless access points.
- Engage in any activity that damages the reputation or digital integrity of SAI University.

6.7 Compliance

Violations of this policy will be considered serious misconduct and may lead to disciplinary action, including suspension of IT privileges, administrative or academic sanctions, termination of employment or enrollment, and/or legal proceedings as deemed appropriate by the University authorities.

7. Protection of Information and Data

7.1 SAI University is committed to maintaining the confidentiality, integrity, and availability of all information and data created, stored, processed, or transmitted using its Information Technology (IT) resources. Every member of the University community shares the responsibility to protect institutional and personal data from unauthorized access, misuse, loss, or disclosure.

7.2 Data Classification

7.2.1 Information handled by the University shall be classified based on its sensitivity and importance. The following categories may be used for classification:

- Confidential Data: Information that is sensitive in nature, including personal records, student grades, research data, financial details, and administrative records.
- Internal Data: Information intended for internal use within the University community, including internal communications, meeting minutes, or drafts.
- Public Data: Information approved for public dissemination, such as press releases,

brochures, or published reports.
7.2.2 All users must handle data in accordance with its classification and ensure that appropriate safeguards are applied.

7.3 Responsibilities of Users

7.3.1 All users are required to:
- Use University data only for authorized academic or administrative purposes.
- Ensure that data is accurate, up to date, and securely stored.
- Protect data from unauthorized access, alteration, or destruction.
- Avoid sharing confidential data with any external party without prior written approval.
- Report any data breach, accidental disclosure, or suspected compromise immediately to the IT Department.

7.3.2 Users must take reasonable precautions such as:
- Using strong passwords and keeping them confidential.
- Logging out of systems when unattended.
- Avoiding storage of sensitive data on unsecured devices or external drives.
- Encrypting data before transferring it through email or external networks.

7.4 Institutional Data Management

7.4.1 The University will implement and maintain appropriate data security measures, including access controls, encryption, backup, and recovery systems.
7.4.2 Data backups shall be conducted at regular intervals to ensure that important information can be restored in the event of system failure, data loss, or cyberattack.
7.4.3 The IT Department shall maintain a Data Retention and Disposal Policy, ensuring that data is retained only for as long as necessary and securely destroyed when no longer required.

7.5 Data Privacy

7.5.1 The University respects the privacy rights of individuals and shall collect, process, and store personal information only for legitimate academic, research, or administrative purposes.
7.5.2 Personal data shall be handled in compliance with applicable data protection laws and regulations, ensuring that consent, confidentiality, and purpose limitations are upheld.

8. Copyrights, Licenses, and Intellectual Property

8.1 SAI University recognizes and upholds the importance of protecting copyrights, software licenses, and intellectual property rights (IPR) in all academic, research, and administrative activities. All members of the University community are required to respect and comply with the laws and institutional policies governing the use of copyrighted and licensed materials.

8.2 Compliance with Copyright Laws

8.2.1 Users shall not reproduce, distribute, or modify any copyrighted material — including text, images, audio, video, software, or databases — without obtaining proper authorization from the copyright holder.
8.2.2 Any use of copyrighted content for educational or research purposes must comply with the provisions of "fair use" or educational exceptions as permitted under applicable laws.
8.2.3 Users are responsible for verifying the ownership and usage rights of all materials used in

university projects, publications, or presentations.

8.3 Software Licensing

8.3.1 All software installed on university systems must be properly licensed and authorized by the IT Department
8.3.2 Users shall not:

- Install or use unauthorized or pirated software on university-owned devices.
- Copy, distribute, or share licensed software beyond the scope of the University's license agreements.
- Alter, reverse-engineer, or attempt to bypass security features of licensed software.

8.3.3 The IT Department shall maintain an updated software inventory and license records to ensure legal compliance and operational integrity.

8.4 Intellectual Property Created at the University

8.4.1 Intellectual Property (IP) developed by faculty, staff, or students in the course of their duties, research, or use of university resources shall be governed by the SAI University Intellectual Property Rights (IPR) Policy.
8.4.2 Ownership of such IP shall normally rest with the University, unless otherwise agreed upon through a specific contract or sponsored research agreement.
8.4.3 Creators are encouraged to disclose any new inventions, software, designs, or research outcomes to the University IPR Cell for protection and registration.
8.4.4 The University supports innovation and shall facilitate patent filing, copyright registration, or technology transfer in accordance with institutional procedures.

8.5 Prohibited Practices

Users shall not:

- Engage in illegal downloading, copying, or distribution of copyrighted works.
- Use University systems for peer-to-peer file sharing involving copyrighted material.
- Claim ownership or credit for intellectual property created by others.
- Remove or alter copyright notices, license terms, or digital rights management information from digital materials.

8.6 Institutional Responsibility

8.6.1 The University will provide awareness and training programs on copyright, licensing, and IPR compliance to all users.
8.6.2 The Director – Information Technology and the IPR Officer shall jointly oversee implementation and monitoring of this policy section to ensure adherence to legal and ethical standards.

9. Social Media and Online Conduct

9.1 SAI University acknowledges the growing role of social media and online platforms in education, research, communication, and community engagement. The University encourages responsible and respectful use of these platforms while ensuring that all online activities reflect the values, integrity, and reputation of the institution.

9.2 Purpose of Social Media Use

9.2.1 The University's social media presence aims to:

- Promote academic excellence, research achievements, and institutional initiatives.
- Facilitate communication and collaboration among students, faculty, and the public.
- Disseminate verified and accurate information about university events, programs, and opportunities.

9.2.2 All users are expected to use social media professionally, ethically, and in accordance with applicable laws and University policies.

9.3 Responsible Online Behaviour

Users of University-managed or personal social media accounts must:

- Communicate respectfully and professionally, maintaining the dignity of the University and its stakeholders.
- Ensure that the information shared is accurate, verified, and free from misinformation.
- Respect privacy, confidentiality, and intellectual property rights in all online interactions.
- Use official University social media accounts only for authorized institutional purposes.
- Obtain prior approval from the Public Relations or Communications Office before posting any official University content or announcements.

9.4 Prohibited Online Conduct

The following actions are strictly prohibited on social media and online platforms:

- Posting or sharing offensive, defamatory, obscene, or discriminatory content.
- Engaging in cyberbullying, harassment, or hate speech.
- Spreading false information, rumours, or unverified claims about the University or any individual.
- Sharing confidential University data, internal communications, or non-public research without authorization.
- Using University logos, names, or branding elements without prior approval from the designated authority.
- Misrepresenting oneself as an official representative of the University on personal social media accounts.

9.5 Academic and Research Integrity Online

9.5.1 Faculty, students, and researchers must ensure that all academic and research-related content posted online:

- Accurately represents research findings and avoids plagiarism.
- Properly acknowledges sources, collaborators, and sponsors.
- Does not violate confidentiality agreements, intellectual property laws, or publication ethics.

9.6 Personal Use of Social Media

9.6.1 While the University respects individual freedom of expression, users are expected to exercise good judgment and digital responsibility when expressing personal opinions online.
9.6.2 Personal views shared on social media must include a disclaimer such as:
"The views expressed are my own and do not represent the official position of SAI University."
9.6.3 Users must ensure that their personal online activities do not damage the University's

reputation or conflict with institutional values.

9.7 Monitoring and Compliance

9.7.1 The University reserves the right to monitor its official social media channels to ensure compliance with institutional guidelines and legal standards.
9.7.2 Violations of this policy may result in disciplinary action, including suspension of access rights, administrative sanctions, or legal proceedings, as deemed appropriate by university authorities.

10. Political and Commercial Activities

10.1 SAI University is an academic and non-profit institution committed to maintaining an environment of neutrality, integrity, and inclusiveness. The University's Information Technology (IT) resources are provided exclusively to support academic, research, administrative, and community service functions. Their use for political or commercial purposes is restricted to protect institutional independence and compliance with legal and ethical standards.

10.2 Political Activities

10.2.1 The University respects the rights of individuals to hold personal political beliefs and to participate in lawful political activities in their private capacity. However, users shall not use University IT resources to:

- Conduct, organize, or promote partisan political campaigns.
- Distribute or circulate political advertisements, petitions, or propaganda through university networks or systems.
- Use University email addresses, logos, or digital platforms for political endorsements or lobbying.
- Host or promote politically affiliated online events or communications using University IT infrastructure, unless formally approved by the competent authority.

10.2.2 Any political activity conducted within the University premises or through its digital platforms must:

- Comply with the laws and regulations of the Government of India.
- Obtain prior written approval from the University Administration.
- Uphold the academic neutrality and non-partisan character of the institution.

10.3 Commercial Activities

10.3.1 University IT resources shall not be used for unauthorized commercial purposes, including but not limited to:

- Advertising, marketing, or selling personal products or services.
- Conducting business transactions or consultancy unrelated to university objectives.
- Sending or hosting commercial messages, solicitations, or promotions using University systems.
- Using University networks for profit-generating online ventures, such as trading, e-commerce, or private entrepreneurship.

10.3.2 Commercial use of IT resources may be permitted only when:

- It directly supports University programs, projects, or collaborative initiatives.
- It is approved in writing by the Chief Finance and Accounts Officer (CFAO) or any designated authority.

- Appropriate reimbursement or cost recovery for such usage is made to the University.

10.4 Sponsorships and External Collaborations

10.4.1 Any collaboration, sponsorship, or partnership involving commercial entities through digital platforms must:

- Be conducted under an official Memorandum of Understanding (MoU) or agreement.
- Be reviewed and approved by the Office of the Registrar and the Legal/Finance Department.
- Ensure that the use of University's name, logo, or brand complies with institutional guidelines.

10.5 Compliance and Enforcement

10.5.1 Any violation of this section, including unauthorized political campaigning or commercial use of IT resources, shall be treated as misuse of university property and may result in disciplinary action.

10.5.2 Depending on the severity of the violation, actions may include:

- Revocation of IT access privileges.
- Administrative or academic disciplinary measures.
- Financial penalties or reimbursement for unauthorized use.
- Legal action as per the relevant laws and University regulations.

11. System and Network Security

11.1 SAI University is committed to maintaining a secure, reliable, and efficient information technology environment. The protection of university systems, networks, and digital assets is essential to ensure the confidentiality, integrity, and availability of institutional and personal data. Every user is responsible for adhering to best practices and institutional guidelines to safeguard IT infrastructure.

11.2 Responsibilities of Users

11.2.1 All users of the University's IT resources are required to:

- Use University systems, servers, and networks responsibly and only for authorized purposes.
- Maintain the confidentiality of passwords and login credentials and change them periodically.
- Log off or lock systems when unattended to prevent unauthorized access.
- Avoid connecting unauthorized devices, USB drives, or personal equipment to university systems without IT Department approval.
- Report immediately any unusual system behaviour, suspected malware, or data breach to the IT Department.

11.3 System Access Control

11.3.1 Access to University systems and data is based on the principle of least privilege—users are granted access only to the information and systems necessary for their roles and responsibilities.

11.3.2 All access credentials, such as usernames, passwords, and digital certificates, are the property of the University and must not be shared or transferred.

11.3.3 User accounts shall be deactivated promptly upon cessation of employment, enrollment, or termination of affiliation with the University.
11.3.4 Remote access to university systems shall be allowed only through secure and authorized channels such as VPNs, with proper authentication controls.

11.4 Network Security and Monitoring

11.4.1 The IT Department shall implement robust network security measures including firewalls, intrusion detection systems (IDS), anti-virus protection, and encryption to protect University systems from unauthorized access or attacks.
11.4.2 All network activities are subject to monitoring and logging for operational integrity, security compliance, and forensic purposes.
11.4.3 Unauthorized attempts to scan, probe, or exploit the University network or systems are strictly prohibited and will result in disciplinary action.
11.4.4 Wireless network access shall be provided only through university-authorized access points, and users must not create personal or ad hoc networks.

11.5 Software and System Maintenance

11.5.1 Only licensed and verified software shall be installed on university-owned systems. Installation or modification of system software must be carried out solely by the IT Department or authorized personnel.
11.5.2 Regular updates, patches, and security upgrades shall be performed to ensure system protection against vulnerabilities.
11.5.3 Users shall not disable or tamper with antivirus software, firewalls, or other protective mechanisms installed by the University.

11.6 Data Backup and Recovery

11.6.1 The University shall maintain a comprehensive data backup and recovery system to safeguard against data loss due to hardware failure, cyberattack, or human error.
11.6.2 Users are encouraged to store critical files and documents on university-approved cloud or server locations rather than local devices.
11.6.3 Data recovery procedures shall be regularly tested and updated by the IT Department to ensure operational readiness.

11.7 Incident Reporting and Response

11.7.1 Any security incident, data breach, or system compromise must be reported immediately to the IT Department.
11.7.2 The IT Department shall investigate, document, and respond to such incidents promptly, in coordination with relevant departments.
11.7.3 Users are expected to cooperate fully in incident resolution, providing all necessary information for analysis and corrective measures.

11.8 Disciplinary Action

11.8.1 Any attempt to bypass security controls, gain unauthorized access, or disrupt network operations shall be considered a serious policy violation.
11.8.2 Such acts may result in:

- Suspension or termination of network and system access privileges.
- Disciplinary proceedings under university rules.
- Legal action as per the Information Technology Act, 2000, and other applicable laws.

12. Privacy and Confidentiality

12.1 SAI University recognizes the importance of protecting the privacy, confidentiality, and integrity of all information stored, transmitted, or processed using its Information Technology (IT) resources. The University is committed to ensuring that personal, academic, research, and administrative data are handled responsibly and in compliance with applicable laws, regulations, and institutional policies.

12.2 Ownership of Data

12.2.1 All data, documents, and digital communications created, stored, or transmitted on university-owned systems, servers, or networks are considered the property of SAI University.
12.2.2 Users are custodians of such data and are responsible for maintaining its confidentiality and security.
12.2.3 Upon cessation of employment, enrollment, or affiliation, users must return or delete any University data in their possession and relinquish all access rights to institutional systems.

12.3 User Responsibility

12.3.1 All users are required to:
- Protect confidential information from unauthorized access, disclosure, or misuse.
- Use University systems only for authorized and legitimate purposes.
- Ensure that sensitive information is encrypted or password-protected before transmission.
- Avoid discussing or sharing confidential University matters through unsecure channels or public platforms.
- Report any data breach, accidental disclosure, or privacy concern immediately to the IT Department.

12.4 Institutional Responsibility

12.4.1 The University shall establish and maintain technical and administrative measures to ensure data privacy and protection. These may include:
- Implementation of access control mechanisms and encryption protocols.
- Regular audits and reviews of data handling practices.
- Controlled sharing of information only with authorized personnel or departments.

12.4.2 The IT Department shall ensure that all digital information stored in university systems is backed up and secured in accordance with institutional data management policies.

12.5 Personal Data and Privacy

12.5.1 The University shall collect, process, and retain personal data of students, employees, and other stakeholders only for legitimate academic, administrative, or operational purposes.
12.5.2 Personal data shall be used in accordance with data protection and privacy regulations, and shall not be disclosed to third parties without consent, except when required by law or for official University functions.
12.5.3 Individuals have the right to access their own personal data, request corrections to

inaccurate information, and inquire about how their data is being used.

12.6 Management's Right to Access Information

12.6.1 While the University respects individual privacy, it reserves the right to monitor, access, or review information stored on its systems when necessary for:

- Investigating misconduct, security breaches, or policy violations.
- Maintaining system performance, compliance, or operational integrity.
- Responding to legal or regulatory requirements.

12.6.2 Such access shall be carried out only by authorized personnel and in accordance with due process and institutional procedures.

12.7 Confidential Information

12.7.1 Confidential information includes, but is not limited to:

- Student records, examination data, and grades.
- Employee records, payroll data, and personnel files.
- Research data, unpublished findings, and intellectual property.
- Financial, strategic, and administrative documents.

12.7.2 Disclosure of confidential information without authorization is a serious violation of university policy and may result in disciplinary or legal action.

12.8 Data Retention and Disposal

12.8.1 Data shall be retained only for the duration required by academic, administrative, or legal needs.
12.8.2 When no longer required, data must be securely deleted or destroyed to prevent unauthorized recovery or misuse.
12.8.3 The IT Department shall maintain a schedule and protocol for secure data disposal in compliance with institutional and statutory requirements.

12.9 Enforcement and Disciplinary Action

12.9.1 Violations of privacy and confidentiality standards will be treated as serious misconduct.
12.9.2 Depending on the severity of the violation, disciplinary actions may include:

- Suspension or termination of IT privileges.
- Administrative or academic penalties.
- Termination of employment or enrollment.
- Legal action under the Information Technology Act, 2000 and other applicable laws.

13. Enforcement and Disciplinary Action

13.1 SAI University expects all members of its community to adhere strictly to the provisions of this Information Technology (IT) Policy. Any misuse, negligence, or violation of the rules outlined herein will be treated as a serious breach of institutional discipline and may attract corrective, administrative, or legal action as appropriate.

13.2 Monitoring and Compliance

13.2.1 The University reserves the right to monitor, audit, and review all use of its IT systems,

networks, and digital resources to ensure compliance with this policy.
13.2.2 Monitoring shall be conducted by authorized personnel of the Information Technology Department in coordination with the Registrar and other relevant authorities, ensuring confidentiality and due process.
13.2.3 The University may collect and review logs, emails, network activities, or stored data when required for operational, security, or investigative purposes.

13.3 Reporting of Violations

13.3.1 Any user who becomes aware of a violation, misuse, or potential breach of this policy shall report the incident immediately to the IT Department or concerned authority.
13.3.2 The IT Department shall review and document reported cases, conduct preliminary investigations, and escalate the matter to the appropriate disciplinary committee or administrative head for further action.
13.3.3 Users are expected to cooperate fully during investigations, providing any relevant information or access necessary for resolution.

13.4 Disciplinary Measures

13.4.1 Depending on the nature and severity of the violation, one or more of the following disciplinary actions may be imposed:

- Written warning or official reprimand.
- Temporary or permanent suspension of access to IT systems and network services.
- Termination of employment or expulsion from the University in cases of severe or repeated violations.
- Financial liability or reimbursement for damages or losses caused by unauthorized activity.
- Referral to law enforcement agencies for criminal or civil proceedings under applicable laws.

13.4.2 In addition to university sanctions, users may also face penalties under the Information Technology Act, 2000, the Indian Penal Code (IPC), or other relevant legislation if their actions constitute a legal offense.

13.5 Appeals

13.5.1 Individuals subject to disciplinary action under this policy have the right to submit a written appeal to the competent authority within the timeframe prescribed by university regulations.
13.5.2 The appeal shall be reviewed by a designated committee, whose decision shall be final and binding.

13.6 Authority and Oversight

13.6.1 The IT in charge shall be responsible for overseeing the implementation and enforcement of this policy in coordination with the Registrar.
13.6.2 The University reserves the right to amend, modify, or update disciplinary procedures to align with emerging technologies, legal requirements, and best institutional practices.

13.7 Awareness and Education

13.7.1 The University shall conduct regular awareness and training programs to educate students,

faculty, and staff about acceptable use, cybersecurity, data protection, and legal implications of IT misuse.
13.7.2 Users are encouraged to remain informed and exercise diligence in maintaining a secure and ethical digital environment.

14. Review and Revision

14.1 SAI University recognizes that Information Technology (IT) systems, digital platforms, and regulatory frameworks evolve continuously. To ensure the relevance, effectiveness, and compliance of this policy, the University shall establish a structured process for its periodic review and timely revision.

14.2 Policy Review Cycle

14.2.1 This policy shall be reviewed at least once every two (2) years, or earlier if necessitated by technological advancements, legislative changes, or institutional requirements.
14.2.2 Interim reviews may be undertaken when:

- New IT infrastructure, applications, or digital systems are introduced.
- Updates in national or international data protection or cybersecurity laws occur.
- Internal audits or security assessments recommend amendments.
- Significant incidents or breaches highlight the need for procedural improvement.

14.3 Review Committee

14.3.1 The review and revision process shall be coordinated by the Information Technology Department under the guidance of the Registrar.
14.3.2 The IT Policy Review Committee shall comprise representatives from:

- The Information Technology Department
- Academic and Administrative Divisions
- Legal and Compliance Office
- Finance Department
- Human Resources Department

14.3.3 The Committee shall evaluate the policy's implementation, effectiveness, and alignment with university objectives and recommend necessary modifications.

14.4 Approval and Implementation

14.4.1 Any proposed amendments or revisions to this policy shall be submitted to the Vice-Chancellor for approval upon the recommendation of the IT Policy Review Committee.
14.4.2 Once approved, the updated policy shall be officially notified to all members of the University community through appropriate communication channels such as circulars, email announcements, or the University website.
14.4.3 The revised version shall supersede all previous editions and become effective from the date of notification.

14.5 Documentation and Record Keeping

14.5.1 The IT Department shall maintain a version-controlled record of all revisions, indicating the date of review, nature of changes, and approval authority.

14.5.2 Previous versions of the policy shall be archived for reference and compliance verification.

14.6 Continuous Improvement

14.6.1 The University is committed to continuous improvement in information security, governance, and technological management.
14.6.2 Feedback from faculty, staff, students, and other stakeholders is encouraged to ensure that this policy remains effective, transparent, and responsive to emerging challenges in the digital environment.

15. Approval

15.1 This Information Technology (IT) Policy of SAI University, Chennai has been reviewed, finalized, and approved by the competent authority of the University to ensure effective governance, secure usage, and responsible management of institutional IT resources.

15.2 The policy has been prepared by the Information Technology Department, reviewed by the IT Policy Review Committee, and endorsed by the Registrar before submission for final approval.

15.3 Upon approval, this policy shall become effective immediately and shall be binding on all members of the University community, including faculty, staff, students, research scholars, contractual employees, vendors, and visitors with authorized access to University IT resources.

15.4 All departments and offices of the University are responsible for ensuring implementation, awareness, and compliance with the provisions of this policy within their respective domains.

15.5 Any amendments, revisions, or related directives shall be issued only with the approval of the Vice-Chancellor or Registrar of the University.