



Information Technology (IT) Policy

Document Type	Policy
Administering Entity	Head – Information Technology (IT), IT Department Staff, Vice-President Administration, Department Heads
Latest Approval/ Amendment Date	10 December 2025
Last Approval/ Amendment Date	15 May 2025
Approval Authority	Board of Directors
Indicative time of Review	9 December 2027

1. Purpose

- a. The purpose of the policy is to ensure the effective protection and proper usage of the information and communication systems of S P Jain School of Global Management (S P Jain / the School).

2. Scope

- a. This Policy applies to:
 - i. all IT resources operated by, used by or provided to all stakeholders by the School
 - ii. all information collected, created, stored or processed on the computer or network resources of the School
 - iii. all individuals who use, deploy and support all IT and network resources provided to all staff, all students, contractors, volunteers and visitors (all collectively referred to as “users”)

3. Roles and Responsibilities

- a. The Head - Information Technology (IT) and staff in the IT Department are responsible for implementing the policy under the oversight of Vice President – Administration.
- b. Managers/Department heads are responsible for ensuring adherence to the IT Policy within their Departments.
- c. The IT Department is responsible for coordinating with the Chief Information Security Officer (CISO) and the Privacy Officer to ensure system-level controls are implemented to support privacy and cybersecurity obligations.
- d. Staff, students, visitors and contractors are required to follow guidelines for safe use of the institution’s IT resources.

4. Computer Systems

a. Network

- i. Network management, administration and maintenance within the School are the responsibility of the IT Department. Access to and usage of the Servers is restricted to authorised members only.
- ii. Students are not allowed to connect to S P Jain's wired network without specific permission from the IT department.
- iii. The wireless network is protected with Wi-fi Keys & other means of identity/authentication system which cannot be shared with other users.
- iv. Internet access will only be provided through the proxy server/content filter server/Firewall. Any exceptions will need permission from the IT Department, which will give permission after ascertaining that the request for access is absolutely necessary.

b. Hardware (PCs, Laptops, Notebooks, Printers, & Peripherals, etc.)

- i. The requirement for IT equipment/facilities will be identified in general within the context of an IT strategy for SP Jain and more specifically within a planned programme upgradation/replacement.
- ii. The purchase, installation, configuration and maintenance of computer equipment is the responsibility of the IT Department.
- iii. Computer equipment/accessory registers will be maintained by the IT Department to ensure full tracking of equipment.
- iv. Requirements for new hardware / software / IT related facilities should be discussed in advance with the IT Manager to assess detailed specifications and security compatibility or policy adherence.
- v. The deployment of new equipment or redeployment of existing equipment is undertaken by the IT Department after consultation with Department Managers/Heads.
- vi. The relocation of hardware within or out of any campus or office premises of the School should be discussed with the relevant IT Manager in advance to ensure good reason for relocation, determine the most appropriate means of relocation and to ensure computer equipment registers are updated.
- vii. The security and safekeeping of portable and other equipment provided by the School is the responsibility of each user.
- viii. Staff members are responsible for the proper usage, care and cleanliness of the computer equipment they use. Managers should ensure that staff maintain the cleanliness of their machines.
- ix. Problems with hardware should be reported to the IT Department in accordance with established IT Help Desk procedures.
- x. Users are solely responsible for the condition and security of all issued devices until they are formally returned to the IT Department. They will be liable for the costs of repair or replacement costs or any other cost involved resulting from any damage, loss, or theft while the hardware is in their possession.

c. Software & Software Applications

- i. The requirement for IT software will normally be identified within the context of an IT strategy for the School and, more specifically within a planned software upgrade programme.
- ii. The purchase, installation, configuration and support of all software and software applications including cloud based SaaS software services to be used within SP Jain are the responsibility of the IT Department/ IT Department's authorised /delegated Services Provider.
- iii. Software utilities etc, must not be downloaded/installed/executed/used by users without prior authorisation from the IT Department. This includes programs downloaded from the Internet or cloud-based web-based / cloud hosted / SaaS applications or any other sources.
- iv. Installation/use of any unlicensed software or software is prohibited.
- v. Software license registers will be maintained by the IT Department to ensure compliance with legislation.
- vi. Requirements for new software/software applications should be discussed in advance with the relevant IT Manager Provider to assess the detailed specification and implications.
- vii. Problems with software should be reported to the IT Department.
- viii. Requests for modifications, enhancements and upgrades of existing software applications should be discussed with the relevant IT Manager.
- ix. Software used by academic staff for academic purposes has to be compatible with The School's existing systems and network and used in consultation with IT department.

d. Data/Electronic Information Back up

- i. Electronic data management and backups should be in accordance with the *Privacy Policy, Records Management Policy, and Information and Cybersecurity Policy* for data retention, disposal, and access control requirements.
- ii. Storage of the School's electronic data at a storage location other than on the School's hardware networks approved/controlled storage location, such as on private cloud, personal email or any other uncontrolled location is prohibited.
- iii. Each individual user is responsible to their manager for the quality of the computer data they have personally processed.
- iv. Department Managers/Heads are responsible for ensuring compliance with the Privacy Policy and any additional local Data Protection legislation with regards to data processed/held within their Department.
- v. All information and data, in any format, created or compiled by staff members in the course of their employment or engagement with the School, including but not limited to documents in any format, emails, contact lists, and designs stored on the School's systems are the sole and exclusive property of the School. Staff members have no personal ownership rights to this data.
- vi. Revealing personal account credentials like password/OTP to others or allowing use of your account by others is prohibited. This includes family and other household members when work is done at home.
- vii. As a condition of employment, staff consent for the examination and use of content, of all data/information processed and/or stored by the staff member on the organisation's systems is required.

e. Back Up

- i. The IT Department is responsible for ensuring the implementation of an effective backup strategy for server held software and data.
- ii. Users of networked desktop PCs should store data on the shared storage server whenever possible. Data stored on local PC may be lost if a problem develops with the PC, and the IT Department may not be able to assist in its recovery.
- iii. Remote and laptop/notebook PC users must ensure they back up their data regularly. The IT Department will provide advice and assistance for the same if required.

f. Anti-Virus Protection

- i. The IT Department is responsible for the implementation of an effective virus security strategy. All machines, networked and standalone, will have up to date antivirus protection.
- ii. The installation of antivirus software on all the School's machines is the responsibility of the IT Department and in case of any absence should be notified to IT department. Students and other users who are using their own computers have to ensure they install updated working & configured antivirus on their computers.
- iii. The IT Department will ensure the upgrade of the system security / antivirus / endpoint protection software on all networked desktop/ laptop and PC's. Any gaps should be notified to IT department.
- iv. Remote users and users of portable machines will assist in the upgrade of antivirus software in accordance with the specified mechanisms agreed with the IT Department.
- v. Staff should virus scan all media (including external disks, pen-drives and CD/DVDs) before their use. The IT Department will provide assistance and training where required.
- vi. On detection of a virus, security incidents, phishing, hacking or any such anomalies, staff should immediately notify the IT Department who will provide assistance for the same.
- vii. Under no circumstances should staff and users attempt to disable or interfere with or try bypassing the antivirus / system protection software's.

5. Computer Users

a. Health and Safety

- i. Health and safety with regards to computer equipment and computer workstations should be managed within the context of the *Health and Wellbeing Policy, Critical Incident Policy* and *Privacy Policy* of the School, and any additional applicable health and safety legislation regarding computer equipment are implemented within their departments.
- ii. The IT Managers will keep abreast of IT related legislation and advise accordingly.

b. Training

- i. It is the responsibility of Department Managers to ensure appropriate computer training for their staff are done. The IT Department will advise and assist on computer related training issues.

c. User Accounts

- i. HR Department Manager should notify the IT Department of new staff members in advance to allow the creation of network/email/other service accounts and system permissions for new staff.
- ii. HR Department Managers should also notify the IT Department of the departure of staff in a timely manner to allow the deletion of IT related services like email accounts/software.

d. User Credentials and Passwords

- i. The IT Department ensures password / any other authentication protection as part of the School's IT system.
- ii. Password and access management should follow the authentication and access-control standards prescribed under the Information and Cyber Security Policy
- iii. Users should change their passwords when prompted by the system in the case of networked machines or on a regular basis for standalone machines.
- iv. Staff are responsible for the security of their account credentials / password which they should not divulge, even to colleagues.
- v. Problems with accounts / passwords should be reported to the IT department / IT Services Provider.

e. System Usage

- i. Users should ensure their computers are fully shut down and turned off at the end of the day.
- ii. Computers should be locked or shut down when left unattended for any significant period.
- iii. With regards to file management, Department Managers will determine the top-level folders/directories and associated permissions for their department and inform the IT Department.
- iv. IT Department will restrict system admin access to all computers owned by the School and deny access/may not install/support software on "user owned" Laptop or mobile devices.

f. Email Systems and Accounts

- i. The School's email system is a core business application. It should not be used for political, business or commercial purposes not related to the School.
- ii. S P Jain's email system must not be used to send illegal or inappropriate material.
- iii. Limited personal use of email is permitted. Managers should ensure there is no abuse of this privilege.
- iv. It is a condition of employment that all staff consent to the examination of the use and content of their email accounts as required.
- v. Transmission of personal data via email must comply with the Privacy Policy and, where applicable, be encrypted or secured as per the Information and Cybersecurity Policy.
- vi. Global distribution lists should be used appropriately. Email to all staff should be used only when appropriate.
- vii. Staff should minimise the unwanted messages in their email inbox to ensure maximum efficiency of the delivery system
- viii. Staff should utilise the archiving facility within the Email system in accordance with current guidelines.

- ix. Any suspected phishing attempts received by staff might be reported to IT departments for prevention or remediations as in accordance with the guidelines.
- x. Confidential material sent by email should be so classified according to guidelines and shared only with caution.
- xi. S P Jain retains the right to access and view all Emails sent and received by the Email system. This right is exercised solely through the IT Department on the instructions of the President and/or staff designated by the President to provide such instructions.
- xii. Staff are prohibited from linking their S P Jain email accounts to personal social media profiles or platforms, except when the content shared on those platforms is directly related to their work duties and has received prior approval from Department Manager/s.
- xiii. Bulk email blasts are not permitted using the School's email platform. Staff must use a designated email marketing or bulk email service, with prior approval from both the IT Department and their Department Manager, for all such communications.

g. Internet

- i. Access to the internet is provided for business purposes. Limited personal use is permitted and is to be restricted to lunch breaks and periods out with working time.
- ii. All internet activity is subject to monitoring for cybersecurity threats and data-leakage prevention in accordance with the Information and Cyber Security Policy.
- iii. Staff should not make inappropriate use of their access to the Internet. They must not use systems to access pornographic, illegal (including VOIP or Peer to Peer software) or other improper material/services according to local laws.
- iv. Users should not use The School's resources to subscribe to chat rooms, dating agencies, messaging services or other online subscription Internet sites unless they pertain to work duties.
- v. SPJSGM retains the right to monitor Internet usage by staff. This right is exercised solely through the IT Department and, where relating to a specific member of staff, only on instructions from a member of Directorate/Appropriate authority.
- vi. It is a condition of employment that all staff consents to the examination of the use and content of their Internet activity as required.
- vii. Abuse of internet access will be dealt with severely, relative to its seriousness. Abuse will lead to removal of the privilege of access from an individual's workstation or dismissal services or referring for further action based on seriousness of the action.

h. Acceptable Use

- i. All users of the School's IT resources must:
 - a. Use IT resources solely for academic, administrative, research, and professional purposes.
 - b. Protect their S P Jain credentials (e.g., usernames, passwords) and avoid sharing them with others.
 - c. Ensure that personal data is handled in compliance with the *Privacy Policy* and system activities conform to the *Information and Cyber Security Policy*
 - d. Comply with all relevant SP Jain policies, applicable laws, and licensing agreements regarding software and digital resources.

- e. Ensure that the School's IT resources are used ethically and in accordance with the university's code of conduct.

i. Non-Acceptable Use

i. All users of the School's IT resources must NOT:

- a. Engage in illegal activities, including hacking, piracy, and unauthorised access to S P Jain's IT systems.
- b. Use S P Jain's IT resources to harass, threaten, or distribute offensive, discriminatory, or inappropriate content.
- c. Disrupt S P Jain's network operations, introduce malware, or engage in activities that compromise IT security.
- d. Use S P Jain's IT resources for unauthorised commercial purposes or personal financial gain.
- e. Share or distribute the School's confidential data without proper authorisation.

6. IT Awareness and Training

- a. The IT department will conduct regular IT training and awareness campaigns and training sessions to keep users informed.
- b. Users must participate in IT training sessions arranged for all faculty, staff, and students.

7. Third-Party IT Services

- a. Any external vendor, service provider or cloud host engaged to deliver IT or data-processing services must comply with the Information and Cyber Security Policy and the Privacy Policy. Such vendors must be approved by the IT Department and the CISO and be contractually bound to maintain confidentiality, lawful processing, and security of data.

8. Control and Monitoring

- a. The School's IT Department monitors IT Resources and information systems for compliance with this policy and related policies of the School.
- b. Monitoring and audit outcomes shall be reported to the Information Security Committee (ISC) for review, as outlined in the Information and Cyber Security Policy.
- c. During the monitoring activity any inappropriate hardware, software and unauthorised access will be removed / disabled.
- d. S P Jain's IT control and Audit methods include:
 - i. Penetration and perimeter testing
 - ii. review appropriate role access and approvals
 - iii. monitor access control (in network firewalls, switches, routers and web filtering tools)

- iv. review the delegation of authority
- v. conduct network audits
- vi. maintain IT accurate records
- vii. conduct IT software audits
- viii. disclosing usage
- ix. monitoring records

e. Non-adherence to / violation of this policy may result in disciplinary actions.

f. The School reserves the right to investigate any suspected misuse of IT resources.

8. Related Policies

- a. Critical Incident Policy
- b. Health and Wellbeing Policy
- c. Privacy Policy
- d. Records Management Policy
- e. Information and Cyber Security Policy

Policy History and Updates Approved by the BOD

Version	Date Executed	Revisions	Approval
1	15 May 2025	New Policy	Board of Directors
2	10 December 2025	<p>Added requirement for the IT Department to work jointly with the Chief Information Security Officer (CISO) and Privacy Officer when handling personal or confidential information.</p> <p>Added stronger cross-reference to the Information and Cyber Security Policy for all backup, data-handling and data-retention procedures.</p> <p>Added stronger acceptable-use obligations requiring compliance with the Information and Cyber Security Policy when accessing, transmitting or storing any personal or institutional data.</p> <p>Added a new section for 'Third-Party IT Services, outlining approval requirements, contractual obligations, and compliance expectations for all external IT providers.</p>	Board of Directors

Version	Date Executed	Revisions	Approval
		Added the requirement for reporting monitoring outcomes and cybersecurity audit results to the Information Security Committee (ISC).	