S P Jain London School of Management	**Acceptable Use of IT policy**
Document Type	Policy
Administering Entity	Chief Operating Officer, IT Support Manager, all staff
Latest Approval/ Amendment Date	4 November 2023
Last Approval/ Amendment Date	27 April 2023
Approval Authority	Board of Directors
Date of review	November 2027

1. Introduction

a. The School's IT facilities must be used responsibly, ethically and legally as well as in accordance with expectations of behaviour. This Acceptable Use of IT policy is intended for all School staff, students and visitors, who use or support the school's information communication and technology (ICT) systems including email, internet and cloud facilities.

b. As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of modern communications, technology and the internet. The policy sets out how the School's computer and network resources are to be used so that the School environment is safe, secure and reliable.

2. Purpose

a. The purpose of an acceptable use policy is to ensure that the facilities provided are used appropriately and only by authorised individuals. The procedures set out in this policy help mitigate cybersecurity risks, avoid users participating in illegal activities, including being drawn into terrorism or accessing illegal material, and reflect the academic integrity and standards of the institution whilst using ICT resources.

b. The objectives of this policy are:

- To encourage safe and responsible use of technology and the internet.
- Avoid violating the law while using the services
- Avoid the viewing or disseminating material that may lead to the member or others being drawn into terrorism or other extremist activities in compliance with the Prevent Policy.
- Ensure that Staff and Student Equity and Fair Treatment policies are observed at all times and that School equipment and internet is not used to harass or abuse others.

3. Scope

a. The School provides access to ICT (Information and Communication Technology) to employees and students for educational and business purposes. This includes but is not limited to academic staff, adjunct faculty, professional services staff, students, alumni, guests and vendors who are using the School's ICT.

b. The resources covered by this policy includes, without limitation:

i. all School owned, operated, leased or contracted computing, networking, telephone and information resources, whether they are individually controlled, shared, standalone or networked; and
ii. all School voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, including email and Microsoft Teams and physical facilities, including all hardware, software, applications, databases, and storage media.

a. The above resources include the resources made available by the SP Jain Global School of Management under the Intercompany agreement between the two organisations.

4. Acceptable use

a. School ICT is provided to specifically for education, training and administrative purposes.

b. Users must use the facilities responsibly and all communications should be professional and courteous.

c. Users should consider the environment and use the resources provided in a sustainable way.

d. Users who are using School assets (Desktop/Laptop) should use equipment and systems as per recommended usage guidelines and take proper care of assets, switch it off properly where applicable.

e. Ad hoc use of School email for personal purposes is permitted but must be reasonable and not disrupt the School's wider IT systems (e.g. spreading of any form of virus or malware), interfere with work or studies of other colleagues and students or harm the Schools's reputation, bring it into disrepute, or incur liability on the part of the School.

5. Unacceptable use

a. Users must not:

i. participate in any online activities or disseminate material that are likely to bring the University into disrepute, create or transmit material that may be defamatory or incur liability on the part of the University, or adversely impact on the reputation of the University.
ii. visit, view, download or communicate any material which contains illegal or inappropriate content. This includes, but is not limited to, pornography, obscene matter, race-hate material, violence condoning messages, criminal skills, or materials which promote acts of violence, or extremist ideologies and activities associated with terrorist groups or cults, gambling or illegal drugs.
iii. use the internet for illegal or criminal activities, such as but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal items including drugs.
iv. use email or other communication methods or view material that is defamatory, or in connection with activities that are bullying or harassing, malicious, discriminatory, offensive or abusive including comments about ethnicity or nationality, gender, disability, age, sexual orientation, appearance, religious belief and practice, political belief or social background.

v. Undertake any violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

vi. Send unsolicited “nuisance” or bulk emails.

6. IT Security

Passwords

a. Passwords should be complex using multiple characters and should not be guessable.

b. Passwords should be change where a suspected security breach has been identified.

c. When away from your computer for a period of time your screen should be locked requiring a password to regain access.

Unacceptable behaviours

a. Users must not

i. share username / password with anyone else. This could result in restrictions being place on the account.

ii. knowingly introduce any form of computer virus to the University’s computer network or seek to gain or hack into restricted network areas.

iii. circumvent user authentication or security of any host, network, or account.

iv. repair or troubleshoot the IT system or grant any access to a third party, in the case of an emergency you must first consult with your HOD or local IT staff.

7 Accessing restricted materials for legitimate reasons

a. There may be circumstances where work or studies require access to or use of materials prohibited under this policy. If so, this should be discussed with the line manager (for staff) or academic supervisor (for students) in advance. In the case of properly supervised or legitimate research purposes, it is acceptable to access such materials following approval by the University’s Research Ethics Committee.

8 **Acceptable Use Policy agreement**

a. Each user must comply with this Acceptable Use Policy and use school resources for educational purposes only.

b. Each user is required to read and understand this policy and sign the applicable Acceptable Use Policy Statement at time of appointment or registration. The signed acknowledgement statement must be maintained by the School. Users who do not sign the Acceptable Use Policy Acknowledgement Statement will be denied access to ICT Systems.

9. Reporting unacceptable use

a. Employees or students who receive emails with inappropriate content from other employees or students or external parties should report the matter to their line manager or academic

supervisor. Similarly if they see that others are viewing and or disseminating inappropriate material this should also be reported.

b. Where the activities or emails relate to extremist ideologies or terrorism groups or activities, these should be reported to the Chief Operating Officer in accordance with the Prevent Group.

c. In the event of inadvertent access to a site serving obviously malicious content, or one suspected of serving malicious content, immediately contact the IT Service Desk.

d. If any malicious software is suspected of being installed on a School device or device accessing School systems you must inform the local IT team immediately.

10. Monitoring

a. The School reserves the right to monitor all staff and student e-mail and internet activity for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Any such monitoring may be related to:

i. ensure operational effectiveness of services
ii. prevent a breach of the law, this policy, or other School policy
iii. investigate a suspected breach of the law, this policy, or other School policy
iv. monitor standards.

11. Access to staff communications and files

a. IT staff who have appropriate privileges have the ability to access all files, including electronic mail files, stored on systems which they manage. Where it is necessary view these files or to intercept network traffic these staff will take all reasonable steps to ensure the privacy of service users.

b. Access to files, including electronic mail files, will only be given to authorised members of staff. Where access to another members files is required, this must be approved by the Chief Operating Officer. Such access will normally only be granted in the following circumstances:

i. where a breach of the law or a serious breach of this or another School policy is suspected
ii. when a documented and lawful request from a law enforcement agency such as the police or security services has been received
iii. on request from the relevant manager, where the managers or co-workers of the individual require access to e-mail messages or files, which are records of a School activity and the individual is unable, e.g. through absence, to provide them

c. After a member of staff leaves the School, files which are left behind on any computer system owned by the School, including servers and including electronic mail files, will be considered to be the property of the School. When leaving the School, staff should make arrangements to transfer to colleagues any e-mail or other computer-based information held under their account, as this will be closed on their departure.

12. Access to student communications and files

a. When a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been

received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct work-based reason for requiring such access.

13. Data Privacy and Disclosure

a. Users must be aware that any personal data which the School holds is potentially disclosable to a requester under any of the applicable Data Protection Legislation including emails and electronic files. Use of IT must be in accordance with the Data Protection Policy.

b. Information and emails may also be disclosed under the Freedom of Information Act

14. Consequences of Breach of the policy

a. In the event of a breach of this Acceptable Use Policy by a User, the School may in its sole discretion:
   i. restrict or terminate a User's right to use the School Network
   ii. withdraw or remove any material uploaded by that User in contravention of this Policy; or
   iii. where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

b. In addition, where the User is also a member of the School community, the School may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance either the Student or the Staff Disciplinary policy.

15. Legal Requirements

a. The School is aware of its legal responsibilities as a higher education institution – particularly in relation to Freedom of Speech under the Human Rights Act (1998) and ensures compliance with:
   i. Computer Misuse Act (1990)
   ii. Copyright, Designs and Patents Act (1988)
   iii. Counterterrorism and Security Act (2015)
   iv. Data Protection Act (2018) and General Data Protection Regulations
   v. Equality Act (2010)

16. Related Documents

- Data Protection Policy
- Freedom of Expression Policy
- Prevent Policy
- Records Management Policy
- Staff code of conduct
- Student Code of Conduct
- Staff Equity, Diversity and Fair Treatment Policy
- Student Equity, Diversity and Fair Treatment Policy
- Staff Disciplinary Policy
- Student Disciplinary Policy
- Staff Social Media Policy