XLRI IT POLICY

XLRI, to accomplish its vision and mission, has initiated a digital learning environment unique in India. As a Digital Institute, we hope to have 24/7 connectivity between students, faculty & staff and other members of the Institute community and their external collaborators. A trusted and effective information technology environment ("IT environment") is vital to the mission of XLRI. IT resources are valuable community assets to be used and managed responsibly to ensure their integrity, confidentiality, and availability for appropriate research, education, outreach and administrative objectives of XLRI. Further, it must maintain the reputation of the Institute without tarnishing the image or violating the dignity of any of its members as a whole and every other IT resources using stakeholder protected under the law of the land.

As a Jesuit Institute, every member guided by this policy must be mindful of the sense of justice, personal dignity and commitment to lawful use of digital resources and every such users of the digital resources should in no way undermine these characteristics of fellow members in and through digital exchanges. Anonymity and impersonation of any kind, harassment, anger, hate, bullying and victimization of any kind in and through digital exchanges is unwelcome and may invite legal action under the law of the land, including but not limited to Information Technology Act 2000 and other such related data protection statutes.

Applicability: This Policy applies to all individuals using XLRI IT resources ("Users"), regardless of affiliation and irrespective of whether these resources are accessed from XLRI's campus(s) or from remote locations.

Within XLRI's IT environment, additional rules, when notified from time to time, may apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks, and to the uses thereof, or to local workplaces, or to specific types of activities. Any rules made therefore must be consistent with this Policy but also may impose additional or more specific requirements or responsibilities on Users as per law of the land, including but not limited to personal data use /protection laws.

XLRI'S DIGITAL RESOURCES

XLRI's electronic information environment is provided to support the Institute mission of education, research and service. The Institute possesses one of the best IT resources for an ICT enabled education platform, with testing labs, digital infrastructure and a high-end data centre.

XLRI was conceived to connect digitally, the students to the Institute through the online platform to meet their learning needs and to provide education innovation in the virtual space. The Institute provides desktops & laptops to all faculty and staff. All the computers are connected to the Campus LAN/ Wi-Fi, which is supported by an Optical Fiber backbone. The campus network covers the Institute's academic block, administrative block, classrooms, library, hostels, faculty and Staff residences. All members of the Institute campus network have access to the internet 24/7.

XLRI Websites: Institute's website hosts public information factually for all stakeholders and therefore should be respected by all, without modifying, altering, substituting, changing or violating any of its content without due authorizations from competent authorities of the Institute.

a) Updates to the websites are to be duly routed through Dean Administration/ Academics Office to the Website Coordinator.

b) Reports on current and future events, on-campus news and authorized public announcements are to be routed through the Dean Administration/ Academics Office to the Website Coordinator.

c) Social media accounts of the Institute are handled by the Media & PR team. Before posting anything on the Institute Website, due approvals are required to be taken from Dean Administration/ Academics Office by the Website Coordinator.

Acceptable Use of XLRI's IT Policy

In keeping with its mission and vision, the acceptable use of XLRI's IT Policy is based on the principle that we safeguard these resources, and everyone assumes personal responsibility for its appropriate and prudent use and agrees to adhere to the policy of the Institute, its regulatory bodies and the IT/Cyber policies/laws of the Government of India.

The term **'Digital Resources'** includes all computing devices (desktop/laptop/palmtop), portable and mobile devices, servers, clients, networks including wireless networks, firewall devices, routers, internet connectivity, internal/external storage devices, hybrid /cloud storage and peripherals like printers and scanners and the collection of software associated therewith.

The users of the Institute's computing, networking and IT facilities are expected to honour & comply with the following rules, intended to preserve the safety, security, and integrity of the whole network. It is intended to preserve the utility and flexibility of the system, protect the privacy and work of students, staff and faculty, and the right to access the international networks to which the system is connected.

The Users of electronic information systems are urged in their own interest to review and understand the contents of this policy made available also on the Institute's web portal. The Institute retains all rights to the entire network and retains all the rights to withdraw, suspend, block or restrict access given to any individual or group if and when circumstances so require.

The IT infrastructure administration will act solely in the interest of the Institute:

a) To protect the integrity, security, or functionality of the Institute and other IT resources.
b) To comply with legal or contractual requirements under law.
c) To investigate alleged or potential violations of law or policy including, without limitation, state, country, the *Bharatiya Nyaya Samhita 2023* or Institute rules, regulations, and policies.
d) To investigate any asserted, threatened or potential complaint or grievance filed or credibly alleged pursuant to law or Institute rules, regulations, policies or subject of law enforcement review or investigation.
e) To protect the Institute from liability or disruption, the Institute may also refer suspected statutory violations to appropriate law enforcement agencies for further investigation or action.

Penalties: XLRI's IT Policy defines penalties for infractions, proportional to the infraction committed, including but not limited to denial of system access, compensational damages for covering losses and employment termination or expulsion from service/employment.

Disclaimer: Every individual user of such IT resources is hereby made aware and notified, that in the event of any act committed in contravention or contrary to the regulations of the Government of India, the Institute will bear no responsibility and/or legal liability for the individual's action and shall not indemnify any such activity. All responsibility lies with the individual for any such acts that may lead to risk of legal liability, both civil and criminal.

In case of any complaints, appropriate action to be taken will be decided and taken by the person in charge of the facility in consultation with the Dean Administration/Academics and/or other authorities of XLRI. An appeal may be made to the Director of the Institute, whose order, which on review of the action taken above, will be final and binding on the individual(s)/group(s).

ACCEPTABLE USE BY FACULTY & STAFF:

Faculty and staff with authorized access to the IT infrastructure and accounts may use the computing and IT facilities for official Institute academic purposes and activities, and for lawful personal purposes if such use

- Does not violate any law of the Country or IT/Cyber act of the Government of India
- Does not violate the Institute IT Policy and generally accepted codes of conduct, even if unstated
- Does not interfere with the performance of the Institute duties or work of an academic nature
- Does not result in commercial gain or private profit
- Does not use it for nefarious purposes
- Accessing/ downloading software applications that have not been procured with valid software licenses by the Institute and hosting unauthorized content

ACCEPTABLE USE BY STUDENTS:

The Institute provides the best of IT facilities for education, learning and research therefore we expect the students to honour the XLRI's IT Policy for one's own good, the good of the fellow student community and other stakeholders.

1. Any attempt to circumvent system security, guess others' passwords, or in any way gain unauthorized access to local or network resources without due approval is forbidden. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or e-mail address while using IT infrastructure provided by the Institute.

2. Transferring copyrighted materials to or from the Institute systems without the express consent of the owner is a violation of international law. In such matters, the Institute bears no responsibility and is not liable in any way for the consequences thereof. In addition, the use of the internet for commercial gain or profit is not allowed from our Institute's educational site. If done so, it will be the sole responsibility of the user to compensate the damages or the loss or the cost to the Institute.

3.   Downloading and installing of new software shall be done with the explicit consent from the IT Manager. Installation of unlicensed software on the Institute hardware /while on the Institute facilities, or on individual machines connected to the Institute network, is strictly prohibited. The Institute provides the Microsoft campus cloud facility which allows students to install authentic software therefore pirated software are not permitted and needs to be eliminated from the machine/systems linked to the Institute's network.

4.   Disruptive use of the Institute's IT resources is not permitted. Persons entrusted with the IT administration of the IT resources will determine whether specific usage is considered normal, excessive, or disruptive and bring it to the notice of the concerned authority.

5.   Computer users must respect the rights of other users. It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. To maintain professional respect, emails intended to a specific person should not be copy-marked to a group. Flaming emails vitiate the learning environment are strictly disallowed. Individuals from where such emails originate shall be cautioned and repeated similar behaviour invites action. Chain letters/ emails are not allowed. Neither is any form of commercial advertising, nor soliciting allowed. Spamming is strictly disallowed. Broadcast messages addressed to group IDs is requested to be used only for academic purposes and emergencies.

6.   In the event of theft/ stolen devices belonging to a student, the Institute is not liable for any loss/damage of devices. The concerned individual is to file an FIR with the police. In case of mobile theft, the SIM is to be blocked immediately. A copy of the report is to be given to IT Manager.

7.   Recreational downloads and peer-to-peer connections for recreational purposes, and games are strictly not allowed on the Institute network. Playing of Games in the IT labs, Library or Classroom IT resources or at any other facilities is strictly prohibited. Internet chat for personal use is banned.

8.   Users are expected to connect only to the official Wi-Fi network of the Institute for Wireless Access for all official purposes. Setting up of unsecured Wi-Fi systems / personal network infrastructure (including hot spots) on the Institute network is prohibited in accordance with the Cyber Law of the Government of India. This includes network devices such as hubs, switches, routers, network firewalls, and wireless access points and these are prohibited.

9.   Display or transmitting of offensive material in any form (either on computer screens or through posters etc.) as reported is strictly disallowed and serious action will be taken against offenders.

10.   **Integrity of Information Resources:** Computer users must not attempt to modify or remove computer equipment, software, or peripherals owned by others without authorization; encroach on others' use of the Institute's information resources or digital information; or intentionally develop or use programs that disrupt other computer or network users.

11.   **Political, personal, and commercial use:** Institute information resources must not be used for political activities. Institute information resources must not be used for personal activities unrelated to the proper functional activities of the Institute. It must not be used for commercial purposes defined as "unrelated Institute business activity".

12. **Deactivation:** Institute provides individual Email IDs to all students who are enrolled in the Institute program. The Email ID is valid/active during a student's tenure at the Institute. The IT department has the right to deactivate/delete the Email ID of any student if it is found to be misused in any manner. The student Email IDs are deactivated by the IT department, who have graduated after a buffer period of 3 months.

ACCEPTABLE DEVICE RULES AT XLRI.

1. All electronic devices, including but not limited to cameras, microphones, audio systems, and laptops, should be used strictly for authorized academic or professional purposes within the institute. Personal use must not interfere with institutional activities or privacy.

2. Recording of any kind (audio, video, or images) is strictly prohibited without prior consent from all individuals involved. This applies to both virtual and physical spaces within the institution.

3. Use of cameras or recording devices in open spaces (e.g., cafeterias, study areas) must comply with privacy norms. Any unauthorized recording in these spaces is a violation of policy and may result in strict disciplinary action by the Institute management.

4. During virtual classes or meetings, the use of devices to record sessions must be authorized by the faculty/facilitator or instructor. Unauthorized recording of these sessions is not permitted.

5. Recordings of lectures or presentations must be conducted only with the approval of the faculty/ facilitator or instructor and with the knowledge of all participants. Unauthorized dissemination of recorded material is prohibited.

6. Unauthorized use of recording devices or non-consensual capturing of images will result in strict disciplinary action, which may include but not limited to suspension or termination of access to institutional resources.

7. In shared areas like meeting rooms, common areas, or outdoor spaces, individuals must adhere to the device policy and respect others' privacy. Any inappropriate use of technology in these spaces will be subject to investigation and appropriate action by the Institute management.

8. CCTV cameras are installed in public or common areas (e.g., corridors, entrances, parking lots) for safety and security purposes. The use of CCTV cameras in private spaces (e.g., restrooms, individual offices) is strictly prohibited.

9. Access to CCTV footage is restricted to authorized personnel only. The footage will be obtained, reviewed, or shared only with the appropriate permissions from relevant authorities (e.g., Dean Administration under the existing CCTV Policy) and strictly for security, safety or legal reasons.

10. CCTV footage will be retained for a predetermined period (currently 90 days) as specified by the institution's data retention policy. After this period, the footage will be securely deleted unless required for ongoing investigations or legal matters.

11. All areas under CCTV surveillance will have visible signage notifying individuals that the area is being monitored for security purposes. This ensures transparency and respects the privacy of those using such public spaces.

12. The policy aligns with applicable privacy and data protection laws. All members of the institution must ensure that their use of electronic devices complies with these legal and ethical standards

13. Any attempt to access, tamper with, or misuse CCTV cameras or their footage without proper authorization will result in strict disciplinary action and such violations shall be subject to appropriate legal consequences under the law of the land, including civil and criminal prosecutions.

14. CCTV footage must be handled with confidentiality and will not be shared, modified, substituted, altered or distributed without appropriate permissions and lawful consents. Its use will be limited to addressing security, health and safety concerns, or in cases wherein, institutional policy or disclosures under law mandates/requires it.

CONSEQUENCES OF XLRI's IT POLICY VIOLATION

Consequences of misuse can include disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. Users are expected to cooperate with system administrators in any investigation. Computing privileges may be suspended or restricted during an investigation; individuals may appeal and petition for reinstatement of privileges through the Dean Administration.

Explanation: Beyond the XLRI IT Policy, violations that come under the ambit of the *Bharatiya Nyaya Samhita 2023 -* The misuse of computer and network privileges such as unauthorized use of another person's identification or password, using the network to send abusive messages, or using computer facilities to interfere with the work of another student or faculty or staff member may be covered under the ambit of the *Bharatiya Nyaya Samhita 2023*. In such cases the Institute shall not be held liable. The liability solely rests with the student, or the individual person and the law will take its own course.

Savings: Notwithstanding anything mentioned herein before, the Institute (XLRI) reserves the right to modify, alter, substitute, change or amend any or all parts of this XLRI's IT Policy, as per the law of the land.

By Order of the Administration.