Acceptable Use Policy (AUP)

Vidyashilp University is committed to providing faculty, staff, students, research scholars, visiting/adjunct faculty, consultants, and authorized users with a secure, reliable, and modern computing and information technology environment to support academic, research, administrative, and institutional activities.

All users of the University's IT resources, including computers, networks, internet services, email systems, cloud platforms, software, storage systems, and wireless infrastructure, are required to comply with this Acceptable Use Policy (AUP). Any violation of this policy may result in disciplinary, administrative, civil, or legal action as deemed appropriate by the University authorities.

1. Scope of Usage

Authorized users may access and use University IT facilities for academic, research, administrative, and limited personal purposes, provided such usage:

- Does not violate University policies, Government of India laws, cyber laws, copyright regulations, or software licensing agreements.
- Does not interfere with teaching, learning, research, administration, or network performance.
- Does not compromise the security, availability, confidentiality, or integrity of University systems and data.
- Does not result in unauthorized commercial activity, private profit, political campaigning, or unlawful activities.
- Does not violate applicable data protection requirements, including the Digital Personal Data Protection (DPDP) Act, 2023, cybersecurity regulations, contractual obligations, or University information security requirements.

2. User Responsibilities

Users are responsible for the proper and ethical use of University IT resources. Users must:

- Use IT resources only for authorized purposes.
- Maintain the confidentiality of their account credentials and passwords.
- Ensure that their activities do not disrupt University operations or negatively impact other users.
- Report any suspected security incidents, unauthorized access, malware infections, or policy violations to the IT Department immediately.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

#125, Bettenahalli, Kundana Hobli, Chapparkallu Road, Bengaluru- 562 110, Karnataka
T. : +91 89511 84990 | E. : info@vidyashilp.edu.in | www.vidyashilp.edu.in

- Exercise responsible and professional conduct while using University digital resources and communication systems.
- Immediately report loss, theft, compromise, or suspected unauthorized access involving University accounts, devices, or institutional data.
- Exercise due care while using Artificial Intelligence (AI) tools and ensure compliance with University policies relating to academic integrity, data protection, privacy, and intellectual property.

3. Account and Password Security

- Users must not share passwords or allow others to access their accounts.
- Users are responsible for all activities carried out using their accounts.
- Passwords must be strong, periodically changed, and not easily guessable.
- Use of another individual's account, impersonation, account forgery, or identity masking is strictly prohibited.
- Shared email or shared login accounts are not permitted unless explicitly authorized by the University for operational requirements.
- Any special-purpose account created for conferences, projects, laboratories, or events must have a designated owner responsible for its usage.

4. Network and System Security

- Any attempt to bypass, probe, exploit, or circumvent system or network security controls is strictly prohibited.
- Unauthorized access to systems, servers, applications, databases, or network resources is prohibited.
- Users must not introduce malicious software, including viruses, worms, Trojan horses, ransomware, spyware, phishing tools, or similar harmful code into University systems or networks.
- Installation or use of unauthorized, pirated, cracked, or unlicensed software is strictly prohibited.
- Downloading or installing software on University-owned systems requires approval from the concerned IT authority or facility in-charge.
- Users must not disable or tamper with antivirus software, endpoint protection tools, firewalls, monitoring systems, or other security mechanisms deployed by the University.
- Systems transmitting passwords or sensitive information must use secure encryption mechanisms such as TLS/SSL.

VIDYASHILP UNIVERSITY * BANGALORE * REGISTRAR

- Connecting unauthorized devices, servers, network equipment, access points, or IoT devices to the University network without approval is prohibited.
- Setting up unsecured Wi-Fi systems, rogue access points, or personal hotspots connected to the University network is prohibited.
- Users shall not use unauthorized VPN services, proxy services, SSH tunnels, anonymization tools, or network bypass mechanisms that circumvent University security controls.
- Installation or use of unauthorized remote access software, hacking tools, vulnerability scanners, password-cracking tools, cryptocurrency mining software, or similar high-risk applications is prohibited unless specifically approved for academic, research, or cybersecurity purposes.
- Users shall cooperate with security monitoring, vulnerability assessments, compliance checks, and incident investigations conducted by authorized University personnel.

5. Internet and Email Usage

- Users should use official University email accounts for all official and academic communications.
- Electronic communication systems must not be used to harass, threaten, defame, abuse, offend, or intimidate others.
- Sending spam, chain mails, fraudulent messages, phishing emails, unsolicited advertisements, or mass communications without authorization is prohibited.
- Subscribing others to mailing lists or external services without their consent is prohibited.
- Broadcast or mass emails may only be sent for legitimate academic, administrative, emergency, or institutional purposes with appropriate authorization.
- Recreational peer-to-peer (P2P) file sharing, unauthorized streaming, or excessive bandwidth-consuming activities that impact network performance are prohibited.
- Accessing, downloading, storing, publishing, or transmitting offensive, obscene, pornographic, hateful, discriminatory, or unlawful material using University IT resources is strictly prohibited.
- Users must exercise caution while opening email attachments, clicking external links, or downloading files from unknown sources.
- Auto-forwarding of University email to personal email accounts or external email services is prohibited unless specifically approved by the IT Department.
- Users shall verify recipient addresses before sending emails containing sensitive or confidential institutional information.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

- Confidential, Restricted, examination-related, student, employee, financial, legal, or research information shall not be transmitted to unauthorized recipients.
- Users shall not upload, transmit, or disclose Confidential or Restricted University information through public Artificial Intelligence (AI) platforms, email-integrated AI assistants, browser extensions, or external AI services without authorization.

6. Data Protection and Privacy

- Users must respect the privacy and confidentiality of institutional, personal, research, and administrative data.
- Unauthorized access, copying, modification, disclosure, or destruction of University data is prohibited.
- Sensitive or confidential information must be stored, transmitted, and shared only through approved and secure mechanisms.
- Users must comply with applicable data protection requirements and confidentiality obligations.
- Academic records, student information, examination content, research data, employee information, financial records, and other Confidential or Restricted information shall be handled in accordance with University policies and applicable legal requirements.
- Users shall access only the information necessary for their authorized responsibilities and shall adhere to the principle of least privilege.
- Confidential and Restricted information shall be stored, transmitted, and shared only through approved and secure systems using appropriate security controls.
- Users shall not store institutional information on personal cloud storage services, personal email accounts, or unauthorized applications.
- Users shall not upload Confidential or Restricted University information to public AI platforms without authorization.
- The University reserves the right to monitor, audit, log, and review network activity, system usage, and electronic communications to ensure policy compliance, operational continuity, and security, subject to applicable laws and regulations.

7. Use of Computing Facilities

- Users are expected to handle all University IT equipment and facilities responsibly and report faults, misuse, or malfunctions promptly to the concerned authority.
- Playing games, cryptocurrency mining, unauthorized media streaming, or excessive non-academic use of University computing facilities is prohibited unless specifically permitted for academic or research purposes.

VIDYASHILP UNIVERSITY * BANGALORE * REGISTRAR

- Users must not engage in activities that may degrade system performance, disrupt services, or negatively affect other users.
- Physical or digital display of offensive, abusive, or inappropriate material within University premises or systems is strictly prohibited.
- Users shall not use University computing resources for cryptocurrency mining, unauthorized commercial hosting, botnets, distributed computing projects, or activities unrelated to approved academic, research, or administrative purposes.
- External storage devices such as USB drives and external hard disks must be scanned for malware before being used on University systems.
- Users shall comply with all software licensing, copyright, and intellectual property requirements while using University computing resources.
- Artificial Intelligence (AI) Usage:
    - Users shall use AI tools responsibly and in accordance with academic integrity requirements.
    - Confidential, Restricted, examination, student, employee, research, financial, or legal information shall not be uploaded to public AI platforms without authorization.
    - AI-generated content submitted for academic or administrative purposes must comply with applicable University policies and disclosure requirements.
    - AI tools shall not be used to violate intellectual property rights, privacy obligations, examination rules, or University regulations.

8. Compliance and Enforcement

- Violations of this policy may be treated as misconduct, indiscipline, misuse of institutional resources, or violation of applicable laws.
- The University may take appropriate action depending on the nature and severity of the violation, including:
    - Issuing warnings or advisories
    - Temporary suspension of network, email, or system access
    - Freezing or disabling user accounts
    - Removal of unauthorized content or software
    - Disciplinary proceedings under University rules
    - Reporting incidents to law enforcement or regulatory authorities where applicable

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE

- In severe or repeated cases, user accounts may be permanently revoked and the matter referred to the University disciplinary committee or appropriate legal authorities.
- Third-party service providers, consultants, contractors, vendors, and external collaborators granted access to University ICT resources shall comply with this Policy and related University requirements.

9. Policy Review and Amendments

Vidyashilp University reserves the right to revise, modify, or update this Acceptable Use Policy at any time in response to technological, legal, operational, or security requirements. Updated policies shall become effective upon notification through official communication channels, including email, website notices, portals, or circulars.

The University may issue supplementary standards, procedures, guidelines, advisories, and security requirements from time to time, which shall be deemed part of this Policy and shall be binding on all users.

VIDYASHILP UNIVERSITY * BANGALORE * REGISTRAR