VIDYASHILP UNIVERSITY

Bring Your Own Device (BYOD) Policy

Vidyashilp University permits the use of personally owned devices such as laptops, tablets, and smartphones for academic, research, and limited administrative purposes, subject to strict compliance with University's IT, Network, Data Protection, Laptop Usage, and Security policies. This policy ensures secure, controlled, and compliant access to institutional resources while protecting University systems and data.

- Personal devices may be used on campus to access University network and digital services only through authorized wired or wireless networks and approved authentication systems subject to compliance with University IT and security policies.
- All BYOD devices must comply with minimum security requirements, including updated operating systems, licensed software, and active antivirus or endpoint protection, as required under the University Network and Security policies.
- Devices must be secured with strong authentication mechanisms such as passwords, PINs, biometrics, or equivalent controls, consistent with the Laptop Usage Policy.
- University data accessed via personal devices must only be stored in approved institutional systems or authorized cloud platforms such as University-managed Google Workspace (Google Drive).
- Storage of sensitive, confidential, or restricted institutional data on personal devices or unauthorized applications is strictly prohibited unless explicitly approved by the competent authority.
- Users must not transfer, copy, or synchronize institutional data to personal storage services, personal email accounts, or unauthorized cloud platforms.
- Users shall not upload Confidential or Restricted University information, student records, employee data, examination content, research data, financial information, or other sensitive institutional information to public Artificial Intelligence (AI) platforms without authorization.
- All BYOD devices must comply with University Network Policy requirements, including prohibition of unauthorized DHCP usage, rogue Wi-Fi connections, VPN bypass tools, and insecure network configurations.
- Personal devices connected to the University network may be subject to authentication, registration, monitoring, and compliance checks as per Network Security Policy.
- Users must not bypass network security controls, firewall restrictions, access controls, or authentication mechanisms when using personal devices.

VIDYASHILP UNIVERSITY * BANGALORE * REGISTRAR

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

- Installation or use of pirated, unauthorized, or unlicensed software on devices used for University access is strictly prohibited as per Software Policy.
- Installation of unauthorized remote access tools, hacking utilities, password-cracking tools, cryptocurrency mining software, network scanning tools, or similar high-risk applications is prohibited unless specifically approved for academic, research, or cybersecurity purposes.
- The University may implement endpoint security, device management, or network access control systems to ensure BYOD compliance and security enforcement.
- Personal devices must not introduce malware, vulnerabilities, or security risks into the University network, and must comply with antivirus and patching requirements under the Security and Laptop Policies.
- External storage devices connected to BYOD devices and used for University work shall be scanned for malware before accessing or transferring institutional data.
- Loss, theft, or compromise of a personal device used for accessing University systems must be reported immediately to the IT Department, especially if institutional data may be affected.
- Users shall immediately change passwords and revoke active sessions where compromise of a device or account is suspected.
- The University reserves the right to block, restrict, or revoke access of any personal device that violates security, network, or data protection requirements.
- Users must ensure that BYOD usage does not interfere with academic, administrative, or network performance of University systems.
- The University is not responsible for loss of personal device, personal data, damage to personal devices, or issues arising from non-institutional storage or usage.
- This policy is aligned with and must be read in conjunction with the University Network Policy, Data Storage and Protection Policy, Laptop Usage Policy, and Software Policy.
- Users shall mandatorily comply with all applicable provisions of the Information Technology Act, cybersecurity laws, and Government of India regulations while using personal devices, besides University's SOPs / Acceptable Use Policy / IT Policy in force.
- Users shall additionally comply with the Digital Personal Data Protection (DPDP) Act, 2023, CERT-In Directions, copyright laws, licensing requirements, and other applicable legal, regulatory, and contractual obligations.
- Violation of this policy may result in suspension of access privileges, disciplinary action, financial liability, or legal proceedings as deemed appropriate by the University.
- These guidelines are subject to periodic review and updates, and any revisions will take effect upon official communication by the University.

VIDYASHILP UNIVERSITY REGISTRAR BANGALORE