



INTERNET, INTRANET & WI-FI ACCESS POLICY

Purpose

This policy establishes the rules and procedures governing the use of Internet, Intranet, and Wi-Fi services within the institution. It ensures secure, equitable, and uninterrupted access for academic and administrative activities.

Scope of the Policy

This policy applies to:

- Faculty & staff
- Students & researchers
- Administrative departments
- Visitors with temporary access
- All devices connected to institutional networks (desktops, laptops, mobiles, IoT devices)

Objectives

- To provide reliable and secure digital connectivity to students, faculty, and staff.
- To regulate access to Internet, Intranet and Wi-Fi resources.
- To safeguard institutional network infrastructure from misuse and cyber threats.
- To ensure compliance with ICT usage standards.
- To promote responsible and ethical use of digital resources within the institution.

General Rules for Internet Access

Access Provisioning

- Internet access is provided primarily for academic, research, and administrative purposes.
- Bandwidth is allocated based on institutional policies.
- Internet usage may be monitored/logged for security (as per IT Act 2000 and CERT-In norms).

Prohibited Activities

The following activities are strictly prohibited:

- Downloading pirated movies, software, or copyrighted materials
- Running proxy servers, VPNs, or anonymizing tools
- Using torrent applications
- Hosting unauthorized websites or servers
- Hacking, port scanning, or network sniffing
- Accessing banned or illegal websites
- Performing activities that violate IT Act 2000

Fair Usage Policy

- High bandwidth activities (streaming, large file downloads) may be restricted.
- Peak-hour controls may be applied.
- Users must avoid excessive or non-academic consumption.

Intranet Access Rules

Intranet Resources

Institutional intranet may include:

- ERP/Samarth portals
- Learning Management Systems (LMS)
- Digital Library resources
- Department servers
- Administrative portals

Access Protocols

- Intranet is accessible only within campus or through institutional VPN.
- Unauthorized access attempts to internal servers are punishable.
- Data stored on intranet systems must follow institutional data privacy rules.
- Users must keep credentials.

Wi-Fi Access Policy

Wi-Fi Registration & Authentication

- Wi-Fi access requires authentication via SSID + user credentials (802.1x/RADIUS).
- Students, faculty, and staff receive unique login credentials.
- Visitors may be provided guest Wi-Fi access with limited bandwidth and validity.

Device Restrictions

- Users may connect only personal devices registered with the IT Department.
- Unauthorized Wi-Fi routers, hotspots, repeaters are prohibited.
- Smart devices/IoT equipment require prior approval.

Usage Rules

- Wi-Fi connectivity shall be used strictly for academic & administrative work.
- Bandwidth misuse or unauthorized bulk downloads will result in access suspension.
- Sharing Wi-Fi credentials is strictly prohibited.
- Students must not use Wi-Fi for illegal, unethical, or harmful content access.