Wi-Fi Network Acceptable Use Policy

Internal Use

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be **University** *u/s 3 of UGC Act, 1956)*

SRM Institute of Science and Technology (SRMIST)

All rights reserved.

This document is meant for exclusive use of SRM IST. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically or otherwise without prior written permission.

RELEASE CONTROL

Version No	Release Date	Details
V 1.0	23-04-2024	First release

POLICY OWNER

Department	Represented by
Office of the Registrar	Registrar

POLICY RATIFIED BY:

Department	Represented by
Directorate of ITKM	IT Steering Committee

POLICY ASSURED BY:

Department	Represented by
All SRMIST Institutions / Directorates / Departments	Deans / Directors / HODs

1. Objective

Usage of Wireless infrastructure at SRMIST is to enhance the accessibility of the internet primarily for academic and research purposes and to access exclusive online resources (licensed online journals) of the University by the SRMIST students/faculty/staff members.

2. Scope

This policy applies to all individuals who are entitled to connect with the SRMIST Wi-Fi network. It is the responsibility of each person to use these services appropriately and in compliance with all University policies.

3. Policy

- The Wi-Fi service is provided via Wi-Fi "access points", which are installed in the majority of buildings in the Kanttankulathur campus.
- Wi-Fi bandwidth is shared by everyone connected to a given access point and/or other wireless devices operating in the same area.
- The Interference may come from personal Wi-Fi hotspots, cordless phones, microwaves, Water coolers, Air conditioners, GSM IBS mobile towers, wireless cameras, wireless video devices and projectors as well as other items using the same radio frequencies (2.5Ghz & 5Ghz) may affect the University Wi-Fi performance.
- Distance from the access point, buildings or objects between your device and the access point, interference, quality of your equipment, the number of wireless devices in the area and other factors may also impact performance.
- The availability of the Wi-Fi signal and its strengths will vary from location to location. Each floor of every block doesn't need to have the same kind of signal strength, coverage and throughput.

- As per the university IT security policy, Users are restricted to accessing the Categories not limited to Illegal Drugs, Pornography, P2P File Sharing, Malware and more vulnerable Sites, Bittrorrent, Spyware, Suspicious content etc.
- As per the university IT security policy users can access the following ports by default:

  Http (80), https (443), ftp (21), POP3 (110), POP3S (995), SMTPS (465), IMAP (143), IMAPS (993), SMTP (587), DNS (53), Whatsapp ports, Telegram ports.
- Access to Wireless internet is only an extended service and neither students nor anyone who is residing in the campus can't demand the service.
- Availability of wireless services solely depends on the discretion of the university and it has the right to stop/interrupt the services at any given point in time.
- The access points installed are the property of the University and any damage or loss of the equipment will be considered a serious breach of the University's code of conduct and disciplinary action will be initiated on the student/s who is found guilty of the loss or damage of the Wireless Infrastructure or the corresponding equipment.
- In the incident of any loss or damage to the wireless infrastructure, ITKM will assess the damage and the same will be recovered from all the students who are residing in that floor/building/hostel.

4. Procedure

- Users can connect with the University wireless network SSID "SRMIST" using their NetID credentials and additional authentication is required to access the internet using the Captive portal URL: https://iac.srmist.edu.in/Connect
- The Telecom Regulatory Authority of India (TRAI), the statutory body that controls the Internet Service Providers (ISPs.) in India directed all Universities to take strong steps in strengthening the security of Wi-Fi networks and the users behind Wi-Fi devices should be registered with authorities and ensure that no other mobile clients, other than registered one, is allowed in Wi-Fi network access.

- The university (as ISP) has the right to do lawful monitoring/logging of all internet users' activity and share it with statutory bodies if warranted. To comply with TRAI's guidelines ITKM implemented the 802.1x-based AAA system to identify the users and their activity.
- Any student or device that accesses Wi-Fi network shall:
    - Protect the user account from unauthorized use by not sharing the credentials with others for any reason/means. You will be held responsible for any misuse of your account.
    - Maximum Number of Concurrent (simultaneous) logins for a user account is THREE devices (either laptop/tablet/mobile).
    - To switch between two devices will take a minimum of 30 minutes after disabling the wireless adapter or switching OFF the already connected devices.
    - Judiciously use the Internet and adhere to other university/hostel policies. Incidents of actual or suspected non-compliance with this policy should be reported to ITKM immediately.

5. Enforcement and Compliance

- The University reserves the right to disable your wireless network access for the following reasons:
    - Allowing other individuals (e.g. friends, co-workers, multiple devices etc.) to use your account.
    - Attempt to tamper/hack the servers/network or overload IT resources and assets by excessive bandwidth usage or misconfigured or knowingly using a false identity.

  - Download/Use/Storing or transmitting illegal copies of copyrighted materials such as patented software/movies/songs etc. is a violation of the regulatory laws that involve the protection of data or privacy.

- Violation of this policy and guidelines is a serious offence and the University shall have the right to permanently seize the laptop/devices and/or initiate strong disciplinary action, including termination from the University if the need arises based on the severity of non-compliance.

- Note: ITKM will provide support only for laptops (having Wi-Fi connectivity issues; not for antivirus/OS/Apps etc.) with legitimate operating systems: Win and Mac; not for all kinds of mobiles/tables and Linux systems.