Acceptable Usage of IT Resources Policy

Internal Use

RELEASE CONTROL

Version No	Release Date	Details
V 1.0	09-05-2019	First release
V 1.1	15-04-2025	Added 3.4.2 regarding using Deepfakes and morphing

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

The computing resources at SRM Institute of Science and Technology (SRMIST) support the educational, instructional, research and administrative activities of the University and the use of these resources is a privilege that is extended to members of the SRMIST community. As a user of these services and facilities, SRMIST members have access to valuable University resources, sensitive data and to internal and external networks. Consequently, it is important for the SRMIST community to behave in a responsible, ethical and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. Individuals need to comply with the Acceptable Usage Policy at all times. Individuals are also subject to Indian central, state, local, cyber and applicable international laws governing many interactions/transactions that may occur through SRMIST Network. The applicability of these laws will change in line with amendments made in these laws as incorporated by their respective governing bodies.

This document establishes specific requirements for using all computing and network resources at SRMIST.

2. Scope

This policy applies to all users of computing resources owned or managed by SRMIST. Individuals covered by the policy include (but are not limited to) permanent and visiting faculty, staff, students, alumni, guests, consultants of the administration, external individuals and organizations accessing network services via central computing facilities.

Computing resources include all the SRMIST owned, licensed or subscribed and leased or managed software and hardware and use of the SRMIST network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the Central Library and Information Technology & Knowledge Management Services), personally owned computers and devices connected by wire or wireless to the SRMIST network, and to off-campus computers that connect remotely to the SRMIST's network services.

2.1.   Your Rights and Responsibilities

As a member of the SRMIST community, the University provides you with the use of scholarly and work-related tools, including access to certain computer systems, servers, software and databases, to the campus telephone, and to the internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a faculty or staff member or a student), and of protection from abuse and intrusion by others sharing these resources.

In turn, you are responsible for knowing the regulations and policies of SRMIST that apply to the appropriate use of SRMIST's computing resources and facilities. You are responsible for exercising good judgment in using the SRMIST's technological and information resources.

As a representative of the SRMIST community, you are expected to respect the University's good name in your electronic dealings with those outside the University. Effective security is a team effort involving the participation and support of every member of the University who deals with information or information systems. It is the responsibility of every computer user to know applicable guidelines and to conduct their activities accordingly.

3. Policy

3.1.   Acceptable Use

The below list provides a framework for activities which are in the category of acceptable use.

1. You should only use the computers, computer accounts, and computer files for which you have authorization.

2. You should not use another users' account or attempt to capture or guess other users' passwords.

3. You are individually responsible for the appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the University for all use of such resources. As an authorised SRMIST user of resources, you should not enable unauthorised users to access the network by using an SRMIST computer or a personal computer that is connected to the SRMIST network.

4. SRMIST is bound by its contractual and license agreements respecting certain third-party resources; you are expected to comply with all such agreements when using such resources. You can't violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations as this will qualify as illegal downloading. Also, installation or distribution of "pirated" or other software products that are not appropriately licensed for use is strictly prohibited.

5. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing SRMIST's network and computing resources. You should make reasonable effort to protect your passwords and to secure resources against unauthorised use or access.

6. You should not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorisation by the system owner or administrator.

7. You should comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

8. You should not use SRMIST computing or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to

disrupt) other computer or network users or damage or degrade performance, software or hardware components of a system.

9. On SRMIST network or computing systems, you should not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically approved and authorised by Directorate of ITKM

3.2.   Fair Share of Resources

Information Technology Services and other University departments which operate and maintain computers, network systems and servers are expected to maintain an acceptable level of performance and must ensure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers, Internet bandwidth and other central computing resources are shared widely and are limited, requiring that resources be utilised with consideration for others who also use them. Therefore, using any automated processes to gain a technical advantage over others in the SRMIST community is forbidden.

The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

3.3.   Adherence with Central, State, Local, Cyber and Applicable International Laws

As a member of the SRMIST community, you are expected to uphold local ordinances and central, state, cyber and applicable international laws. SRMIST guidelines for using technologies derived from this concern, including laws regarding license, copyright and the protection of intellectual property. As a user of SRMIST's computing and network resources, you must:

1. Abide by all Central, State, Local, Cyber and applicable International Laws.

2. Abide by all applicable copyright laws and licenses. SRMIST has entered into legal agreements or contracts for many of our software and network resources, which require each individual using them to comply with those end-user agreements.

3. Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and the production of electronic information as the ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorised access, invasion of privacy and copyright infringement.

4. You should not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

5. You should not use SRMIST computing and network resources for illegal activities

3.4.   Other Inappropriate Activities

1. Use SRMIST's computing facilities and services for those activities that are consistent with the educational, research and public service mission of the University. Other prohibited activities, but by no means exhaustive, include:

   - Activities that would jeopardise the University's tax-exempt status.

   - Use of SRMIST's computing services and facilities for political purposes.

   - Use of SRMIST's computing services and facilities for personal economic gain.

2. University IT infrastructure shall not be used to create, modify, or distribute:

   - Deepfake videos, morphed images, or AI-generated media that mislead, impersonate, or cause harm.

   - Content that violates privacy, spreads misinformation, or breaches University policies / applicable laws.

- Any unauthorized modifications to university-related materials, such as ID cards, certificates, or faculty recordings.

- If the act involves cybercrime, defamation, or privacy breaches, legal action may be taken as per applicable laws.

3.5.   Privacy and Personal Rights

- All users of the SRMIST's network and computing resources are expected to respect the privacy and personal rights of others.

- You should not access or copy another user's email, data, programs, or other files without the written permission of the respective user.

- You are expected to be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to disciplinary action by the Registrar of SRMIST as well as legal action by those who are the recipient of these actions.

- **Privacy in Email**: While every effort is made to ensure the privacy of SRMIST's email users, this may not always be possible. In addition, since faculty and staff members are granted the use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from authorised offices, reserves and retains the right to access and inspect stored information without the consent of the user.

3.6.   Enforcement

For security and network maintenance purposes, authorised members within IT services can monitor equipment, systems and network traffic at any time. ITKM reserves the right to audit networks and systems, as required to ensure that SRMIST is not subject to claims of institutional misconduct and to determine if an individual is in violation of this policy. If an individual is found to be in violation of this policy, the concerned authority of SRMIST will take disciplinary action, including the restriction and possible loss of network

privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University.

Access to files on University-owned equipment or information will only be approved by specific members when there is a valid reason to access those files. Authority to access user files can only come from the Directorate of ITKM in conjunction with the Vice Chancellor and Registrar. External law enforcement agencies and Public Safety may request access to files through valid subpoenas and other legally binding requests. The Registrar must approve all such requests in conjunction with the legal department.

Information obtained in this manner can be admissible in legal proceedings or in a University hearing.

3.7.   User Compliance

When you use University computing services and accept any University-issued computing accounts, you agree to comply with this and all other computing-related policies. You have the responsibility to keep yourself up-to-date on changes in the computing environment, as published, using either University electronic or print publication mechanisms, and to adapt to these changes as necessary.