SREE SWAMY VIVEKANANDA CENTRE OF TEACHER EDUCATION

Policy on Acceptable Use of Technology

Executive Summary

This document outlines the terms and conditions governing access to the network and computing resources at Sree Swamy Vivekananda Centre of Teacher Education (hereafter referred to as the "Institute"). All users, including students, employees, contractors, consultants, and any individuals affiliated with third parties, must adhere to the stipulations set forth in this policy. Failure to comply with this policy may result in access restrictions or disciplinary actions.

Key Points:

1. The laws of the jurisdiction in which the Institute is located regarding the use of technology and devices take precedence in cases of disputes. This policy serves as a set of guidelines and should be interpreted in accordance with applicable laws.
2. The primary purpose of our computing and network resources is to support academic activities. In cases of conflicting interests, academic usage will take precedence over non-academic needs.
3. Each individual is provided with a login account, enabling access to network and other resources. Users are responsible for all activities conducted through their accounts, including any unauthorized or unlawful actions.

Protect your account by not sharing your password with anyone, even friends or family members.

4. Unauthorized use of another person's account, with or without permission, is strictly prohibited and may result in the suspension of both users' accounts.
5. Public access machines, such as those in computer labs, must not be used for downloading or storing objectionable materials that may be offensive to other users.
6. Sharing or hosting illegal or objectionable material is forbidden and will result in appropriate penalties, including potential disciplinary action or referral to legal authorities. Any legal consequences arising from such misuse will be the sole responsibility of the individual involved.

Purpose

The purpose of this policy is to establish the acceptable use of computer equipment and network resources at Sree Swamy Vivekananda Centre of Teacher Education. These guidelines are designed to protect the Institute and its users from risks such as security breaches, virus attacks, and legal complications associated with inappropriate technology use.

Scope

This policy applies to all members of the Institute community, including students, employees, contractors, consultants, and individuals associated with third parties. It encompasses all equipment owned or leased by the Institute, as well as privately owned equipment connected to the Institute's network services.

Policy

General Use and Ownership

1. While the Institute values user privacy, it is essential to understand that users are responsible for the security and confidentiality of data stored on their equipment. The

Institute cannot guarantee the privacy of information on network devices owned by the Institute.
2. Users are expected to exercise good judgment regarding personal use of the network. Individual departments may establish specific guidelines for personal internet use. In the absence of departmental policies, users should adhere to Institute guidelines on personal use.
3. For security and network maintenance purposes, authorized individuals within the Institute may monitor equipment, systems, and network traffic as needed.
4. The Institute reserves the right to perform periodic audits of networks and systems to ensure compliance with this policy.

Security and Proprietary Information

1. Users must keep their passwords secure and not share their accounts. System-level passwords should be changed quarterly, while user-level passwords should be changed every six months.
2. PCs, laptops, and workstations should be secured with password-protected screensavers set to activate within 10 minutes of inactivity or by logging off when not in use.
3. Users must take precautions when using public machines and delete personal information before logging out.
4. Hosting or sharing files for download by others is not permitted.
5. Any postings to newsgroups from an Institute email address should include a disclaimer that the opinions expressed are the individual's own and not necessarily those of the Institute, unless the posting is part of official duties.
6. All hosts connected to the Institute's network must have approved virus-scanning software with up-to-date virus databases.
7. Users should exercise caution when opening email attachments from unknown senders, as they may contain viruses or other malicious content.

Unacceptable Use

The following activities are strictly prohibited and are subject to disciplinary action:
System and Network Activities
1. Violations of intellectual property rights, including copyright, trade secret, and patent laws.
2. Unauthorized copying or distribution of copyrighted materials, including software, music, and images.
3. Possessing or distributing material that violates an individual's privacy or other rights.
4. Exporting software or technical information in violation of international or regional export control laws.
5. Introducing malicious programs into the network or servers, such as viruses, worms, or Trojan horses.
6. Sharing account passwords or allowing others to use one's account.
7. Using Institute resources for activities that violate sexual harassment or hostile workplace laws.
8. Making fraudulent offers or statements on behalf of the Institute.
9. Posting statements about warranties, unless part of regular job duties.
10. Causing security breaches or disruptions of network communication.
11. Port scanning or security scanning without prior notification to the Institute.
12. Engaging in network monitoring that intercepts data not intended for the user's host.
13. Circumventing user authentication or security measures.
14. Interfering with or denying service to other users.
15. Sending messages or using programs with the intent to disrupt a user's terminal session.

Email and Communications Activities

1. Forwarding email from Institute-hosted mailing lists to outsiders without explicit consent.
2. Harassment through email, telephone, or paging.
3. Sending unsolicited email or spam.
4. Unauthorized use or forging of email header information.
5. Solicitation of email for harassing purposes.
6. Creating or forwarding chain letters, Ponzi schemes, or pyramid schemes.
7. Using Institute resources to post non-business-related messages to a large number of Usenet newsgroups.

Blogging

1. Blogging from Institute systems or personal computers should be done professionally and responsibly.
2. Confidential information, trade secrets, or proprietary information must not be disclosed in blogs.
3. Blog content should not harm the Institute's image or reputation and should not contain discriminatory, defamatory, or harassing comments.
4. Bloggers must not represent themselves as Institute employees unless explicitly authorized.
5. Institute trademarks, logos, and intellectual property may not be used in connection with blogging activities.

Enforcement

Violations of this policy may result in disciplinary actions, including termination of enrolment or employment, as determined by the Institute's Disciplinary Committee.