Section: 500 – Facilities	Subject: 560- Operations and Maintenance
Policy: Information Technology Acceptable Use	Approved: August 3, 2021
Policy #: CCS 562.07	
Approved: Susan Huard, Interim Chancellor	Effective Date: August 3, 2021

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. Policy Statement

Information technology resources are used by individual employees, students, and other persons affiliated with the Community College System of New Hampshire (CCSNH) and its Colleges. These resources are to be used for educational and business purposes in serving the interests of CCSNH and its Colleges. Misuse of information technology resources poses legal, privacy and security risks and therefore it is important for all users to understand the appropriate and acceptable use of such resources. Effective security and protection is a team effort. It is the responsibility of every user to know this policy, the standards contained herein, and to conduct their activities accordingly.

II. Policy Purpose

This policy establishes the proper use of CCSNH information technology resources and makes IT Users aware of what CCSNH deems as acceptable and unacceptable use.

III. Scope of Policy

This policy applies to employees, students and any other person who has access to CCSNH information technology resources including computers, email, Internet, social media, the network and any other CCSNH information technology or storage system (collectively "IT Users"). All IT Users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CCSNH policy and standards.

IV. Privacy

CCSNH reserves the right to monitor, duplicate, record, and/or log all use of CCSNH technology resources with or without notice. This includes, but is not limited to, email, Internet access, file access, logins, and/or changes to access levels. **IT Users shall have no expectation of privacy in the use of CCSNH technology resources.**

V. General Use, Access and Ownership

5.1 CCSNH Information Assets stored on electronic and computing devices, whether owned or leased by CCSNH, employees, students, or a third-party, remain the property of CCSNH. Computer and telecommunication equipment, software, operating systems, storage media, Intranet, network accounts providing electronic mail, Internet access and browsing, and related network systems, are the property of CCSNH. These systems are to be used for educational and business purposes serving the interests of CCSNH and its Colleges.

5.2 **Access to CCSNH technology resources is a privilege not a right**. CCSNH technology resources include, but are not limited to, computers, equipment, email, Wifi, Internet access and browsing, Intranet, social media, telecommunications and network services, video network services, web services, software, applications, printing and scanning services, and user and technical support provided by Information Technology Staff. Accepting access to any CCSNH technology resource carries an associated expectation of responsible and acceptable use. Failure to meet the standards set forth herein or constitutes a violation of this policy and may result in disciplinary action up to and including termination or denial of access, termination of employment or, for students, dismissal from the College.

5.3 IT Users may access, use and share CCSNH Information Assets only to the extent and for such purposes that access is authorized. This policy expressly prohibits accessing or attempting to obtain unauthorized access, supplying false or misleading information to access, and circumventing user authentication or security of any host, network or account. IT Users are prohibited from accessing data not intended for the IT User, logging into a server or account without express authorization, and probing the security of systems or networks without express authorization.

5.4 An IT User's access to technology is not transferable. Access privileges may not be shared with any other person.

5.5 IT Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of CCSNH Information Assets.

5.6 CCSNH reserves the right to immediately, and without prior notice, disconnect any system or terminate any user access to protect the security of CCSNH technology resources, CCSNH Information Assets, and CCSNH IT Users.

VI. Password Security and Protection

6.1 Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network. CCSNH has established the following standards for password security and protection.

6.2 IT Users must create passwords that:

- Contain a minimum of 14 characters and a maximum of 64 characters. Passwords may contain or be any combination of the following:
- Both upper and lower case letters.
- Contain numbers (for example, 0-9).

- Contain special characters (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

6.3 IT Users should not create passwords that:

- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

6.4 IT Users should not write passwords down or store them anywhere in their office or in a file on a computer system or mobile devices (phone, tablet) without encryption. Instead, IT Users should create passwords that can be remembered easily. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

6.5 All system-level passwords (for example: root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

6.6 All user-level passwords (for example: email, web, desktop computer, and so on) must be changed at least once a year.

6.7 Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers, and family members. All passwords are to be treated as sensitive, confidential CCSNH information.

6.8 Passwords must not be inserted into email messages or other forms of electronic communication or saved using the "Remember Password" feature of applications (for example, Internet browsers).

6.9 Any IT User suspecting that his/her password may have been compromised must report the incident and change all passwords.

VII. Unacceptable Use

7.1 System and Network Activities

The following activities are strictly prohibited:

7.1.1 Connecting computers or other devices directly to the CCSNH network that have not been registered with, or approved by, CCSNH.

7.1.2 Installing software or hardware on or modifying the software or hardware configuration of a CCSNH-owned IT asset without appropriate authorization from CCSNH Chief Information Officer.

7.1.3 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CCSNH.

7.1.4 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCSNH or the end user does not have an active license is strictly prohibited.

7.1.5 Violation of federal, state or local laws and regulations regarding access and use of information resources (*e.g.*, Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Computer Fraud and Abuse Act, code of professional conduct, etc.).

7.1.6 Except for Internet browsing, accessing data, a server or an account for any purpose other than CCSNH educational or business purposes, even if access is otherwise authorized, is prohibited.

7.1.7 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate CCSNH official should be consulted prior to export of any material that is in question.

7.1.8 Introduction of malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, email bombs, etc.)

7.1.9 Using a CCSNH technology resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and policies.

7.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data that the IT User is not an intended recipient of or logging into a server or account that the IT User is not expressly authorized to access. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7.1.11 Using any kind of program, script, or command designed to interfere with a user's computer or network session or collect, use or distribute another user's personal information.

7.1.12 Port scanning, security scanning and executing any form of network monitoring that will intercept data not intended for the IT User's host.

7.1.13 Circumventing user authentication or security of any host, network or account.

7.1.14 Introducing honeypots, honeynets, or similar technology on the CCSNH network.

7.1.15 Interfering with or denying service to any user other than the IT User's host (for example, denial of service attack).

7.1.16 Providing information about, or lists of, CCSNH employees or students except as expressly authorized.

7.2 Email and Communication Activities

CCSNH faculty and staff must use their assigned CCSNH email address for all email communication to students and other official business of CCSNH and its Colleges. CCSNH faculty and staff shall not forward CCSNH email to personal email addresses.

When using CCSNH technology resources to access and use the Internet, users must realize that their communications may be viewed as representing CCSNH unless they clearly indicate otherwise.

The following activities are strictly prohibited.

7.2.1 Sending unsolicited email messages including sending "junk mail," chain letters, Ponzi or other pyramid schemes of any type, or other inappropriate use of email distribution lists.

7.2.2 Any form of harassment via email, telephone or texting, whether through language, frequency, or size of messages.

7.2.3 Unauthorized use, or forging, of email header information.

7.2.4 Unauthorized use of CCSNH and its Colleges registered Internet domain names.

7.2.5 Solicitation of email for any other email address, other than that of the sender's account with the intent to harass or to collect replies.

7.3 Blogging and Social Media

7.3.1 CCSNH employees who engage in blogging or use social media, whether using CCSNH's technology resources or personal computer systems, should at all times be accurate, should exercise appropriate restraint, should show respect for the opinion of others, and should make every effort to indicate when the CCSNH employee is and is not an institutional spokesperson.

7.3.2 When an employee is expressing his or her beliefs and/or opinions in blogs or social media, the employee may not, expressly or implicitly, represent themselves as a representative of CCSNH or its Colleges.

7.3.3 The name, seal, images and other insignia of CCSNH or any of CCSNH's Colleges shall not be used without the express written permission of CCSNH.

7.3.4 CCSNH hosted web pages and blogs are not to be used for activities unrelated to the business purposes or educational mission of CCSNH or its Colleges without prior written authorization.

7.3.5 CCSNH IT Users are prohibited from revealing any CCSNH confidential or proprietary information, trade secrets or any other Restricted Internal, Confidential or Private Information when engaged in blogging or use of social media.