February 22, 2016

Granite State College

Computer & Network Acceptable Use Policy

Part 1

I. Introduction

This acceptable use policy governs the use of computers and networks at Granite State College (GSC). Users are responsible for reading and understanding this document. This document protects the consumers of computing resources, computing hardware and networks, and system administrators.

II. Rights and Responsibilities

Computers and networks can provide access to resources on and off GSC locations, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

III. Computer equipment and property

GSC assigned computers are intended to be used for college-related business as a productivity tool and for research and communication. They are not intended as a replacement for any computers an individual may own personally. Use of college networks and computer equipment for personal purposes should be limited, in compliance with the college's published policies, and in compliance with the terms and conditions of applicable software license agreements.

While computer equipment is provided for an employee's use, it remains the property of Granite State College. In the event that a mobile device is lost, stolen or damaged, financial coverage will normally be borne by the College. However, it is the employee's responsibility to take appropriate precautions to prevent damage to or loss/theft of the assigned equipment. The employee may be responsible for certain costs to repair or replace the computer if the damage or loss is due to negligence or intentional misconduct. Policies for appropriate use of college property may be used to determine whether liability due to negligent behavior exists. Should assigned equipment be lost or stolen, a report of the disappearance must be made to the proper authority immediately.

Sensitive data (i.e. Social Security Numbers, confidential information, etc.) should not be stored on the laptop computer or on a portable data storage device. Employees must abide by the college policies for appropriate use of software, including the requirement to provide legal license to a program before it can be installed on a college-owned computer.

Each laptop is labeled with a unique property ID. The property ID allows IT to manage laptop assignments, coordinate repairs, and maintain systems. Please do not remove the property ID tag from your laptop. The College and IT will secure, via warranty extension or other means, the services needed to repair the laptop should its operation be impaired by a component failure or normal wear and tear.

The laptop will be password protected and will have encryption, antivirus, and/or other data security applications installed. These tools are in place to best protect sensitive data and other college-related information that may be stored on the assigned laptop. These applications and tools must be not be disabled.

Theft or loss that occurs while at a GSC location should be reported to the IT Service Desk. For theft or loss off-site, you should report the disappearance to the local police and to the IT Service Desk. The police report should include the serial number for the lost computer. Provide the IT Service Desk with a copy of the police report within 48 hours of the discovery of the loss. The IT Office will inform USNH Internal Audit of the loss.

The laptop will be configured with wired and wireless connectivity to the Internet. Although IT may offer some tips or advice about best practices for off-site use, it will be up to you and your ISP to make remote connections work. Should you have problems with your laptop, contact the IT Service Desk for hardware repair, software installation or problem diagnosis. IT staff will not visit your home to provide services.

Laptop computers are cycled for refresh after four years. IT will perform operating system and application software upgrades during this period

Documents stored on college issued laptops are not backed up. Damage or corruption of the computer drive could lead to permanent loss of data stored only on the laptop disk drive. For security, confidentiality, and reliability, IT recommends storing all documents on network drives. These drives are accessible from all GSC campus locations and from off-campus locations through VPN connections." It would be prudent to establish a process of copying the data files you use on the laptop to your central data storage area (i.e., your assigned individual server folder) as an added precaution against data loss. Server storage should not be used to backup personal documents or data files, such as personal photos, music, or video. The majority of computers redirect the local documents folders to server locations. Please contact the IT Service Desk if you are unclear about the safety of your files.

IV. Existing Legal Context

All existing laws (federal, state, and/or local) and GSC/University System of New Hampshire regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. This document expands upon USNH policy applicable to Granite State College. Please refer to University System of New Hampshire policy on Operation and Maintenance of Property (USY.VI.F.1.1). The USNH policy document can be viewed at http://www.usnh.edu/policy/usy/vi-property-policies/f-operation-and-maintenance-property in sections 4 through 7. Users do not own accounts on GSC computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (Title 18 U.S.C. section 2510 et. seq.), users are entitled to privacy regarding information contained on these accounts. This act, however, allows system administrators or other GSC employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the College. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search and seizure by law enforcement agencies in compliance with a valid court order. Note: student files at computer facilities are considered "education records" under the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. section 1232g). This Act requires notice and written consent by the student before a personal record can be provided to a third party other than officers of the institution attended by the student or as permitted by law. Misuse of computing, networking or information resources may result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable GSC/University System of New Hampshire policies and/or procedures. Illegal production and/or reproduction of software and other intellectual property protected by U.S. copyright law are subject to civil damages and criminal punishment including fines and imprisonment. Other organizations operating computing and network facilities that are reachable via the College network may have their own policies governing the use of those resources. When accessing remote resources from GSC facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

V. Enforcement

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the accounts or network. Repeated minor infractions or serious misconduct may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to: unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, harassment, or threatening behavior. Any offense that violates federal, state and/or local laws may result in the immediate loss of all GSC/University System of New Hampshire computing privileges and will be referred to appropriate College administrators and/or law enforcement authorities. These are circumstances when a user’s access to IT resources may be deactivated or terminated or expectations of privacy may be waived under the following special conditions which fall under the procedural safeguards found in the USNH Online Policy Manual, http://www.usnh.edu/policy/usy/vi-property-policies/f-operation-and-maintenance-property (see sections 4 through 7)

- Diagnosis: when necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of IT resources
- As required by law: when required by federal, state, and/or local law or administrative rules
- Reasonable grounds: when there are reasonable grounds to believe that a violation of law or policy may have taken place and access and inspection or monitoring may produce evidence related to the violation
- Essential business: when such action to IT resources is required to carry out essential business functions of the College

User accounts posing a threat of security breach, network or system disruption, harassment, threat, or unlawful action, may be immediately terminated to avoid further risk from the account. The account may be enabled pending mitigation of the threat or violation. Consultation with the account owner, and depending on the nature of the issue, with the supervisor, Human Resources department, Academic Affairs office, or Title IX coordinator, may be required before restoring account access.

Complaints of Alleged Violations: An individual who believes that they are harmed by an alleged violation of USNH policy or GSC Computer Acceptable Use policy may file a complaint with the IT Service Desk or the CIO at GSC for review and action. In addition, the individual may also report the alleged violation to other appropriate GSC officers.

Reporting Observed Violation: If an individual has observed or is aware of an alleged violation of this policy, they may report this to the IT Service Desk or the CIO.

Disciplinary Procedures: When informal processes do not, or cannot, resolve the infraction(s), alleged violations will be pursued in accordance with the appropriate disciplinary procedures established for students, faculty, and staff. The HR department and the individual's supervisor, Academic Affairs, or the Title IX coordinator may conduct formal or informal proceedings. The CIO or his/her designee may participate as necessary.

Appeals: Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance to established GSC policy and procedures.

VI. Conduct

Conduct which violates this policy includes, but is not limited to the activities in the following list:

- Unauthorized use of a computer account. Using or attempting to use the account of another user.
- Sharing or distributing account passwords, including your own password.
- Using the GSC/University System of New Hampshire network to gain unauthorized access to any computer systems.
- Connecting unauthorized equipment to the GSC/University System of New Hampshire network.
- Disabling antivirus or encryption on college computers.
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes running programs to identify vulnerabilities or scan networks and computers, intercept data on computers or networks, or to decrypt intentionally secure data
- Using remote access software or proxy systems to bypass firewall protections.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer

system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Deliberately wasting/overloading computing resources, such as printing too many copies of a document.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
- Using GSC/University System of New Hampshire resources for commercial activity such as creating products or services for sale.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming"
- Forging the identity of a user or machine in an electronic communication.
- Transmitting or reproducing materials that are harassing, slanderous or defamatory in nature, or that otherwise violate existing laws or GSC/University System of New Hampshire regulations.
- Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Note: This policy has been adapted with permission from the University of California, Davis “Computer and Network Use Policy” and the “Acceptable Use Policy for Informational Technology Resources at the University of New Hampshire.”