USNH ACCEPTABLE USE POLICY
OVERVIEW AND MAPPING

OVERVIEW

The new USNH Acceptable Use Policy consolidates existing policy provisions from the institutional AUP/CNUPs into a single, comprehensive, USNH-wide Policy that defines acceptable use of information technology resources for all USNH institutions and community members.

MAPPING TO CURRENT POLICIES

The new USNH Acceptable Use Policy does not fundamentally change the intent of the existing institutional policies defining acceptable use of information technology resources. It pulls from all four of the institutional policies to create a comprehensive and inclusive system-wide Policy. Additionally, the new Policy contains:

- Updated language to reflect current, consistent terminology across all Cybersecurity Policies & Standards
- Adjusted responsibilities to address organizational changes
- Explicit Policy requirements in place of vague or general provisions
- Provisions written at the appropriate level of detail, moving implementation or compliance details to the related Standards, where they belong

The following institutional policies will be replaced in full by the new USNH Acceptable Use Policy. A complete mapping of each impacted policy’s provisions to the new Policy is provided below.

- GSC – Computer & Network Acceptable Use Policy
- KSC – Computer and Network Use Policy
- PSU – Acceptable Use Policy (FIN-001)
- UNH – Acceptable Use for Information Technology Resources

A list of all new provisions introduced by this Policy for each institution is provided in that institution’s High Level Mapping document.

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Acceptable Use Policy and/or the relevant USNH Cybersecurity Standards.

- *Italics* = existing Policy language
- NP = USNH Acceptable Use Policy section
- ST= USNH Cybersecurity Standard
- Removed = provisions that are not being carried forward at this time
GSC - COMPUTER & NETWORK ACCEPTABLE USE POLICY


4.1 Introduction. This acceptable use policy governs the use of computers and networks at Granite State College (GSC).

- **NP** = Section 2

Users are responsible for reading and understanding this document.

- **NP** = Section 3

This document protects the consumers of computing resources, computing hardware and networks, and system administrators.

- **NP** = Section 1

4.2 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.

- **NP** = Section 4.2 and 4.1.2

4.3 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.

- **ST** = Endpoint Management Standard

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.

- **NP** = Section 4.7

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.

- **ST** = Endpoint Management Standard
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.

- **Removed, inconsistent with existing Policy at other institutions**

Should assigned equipment be lost or stolen, a report of the disappearance must be made to the proper authority immediately.

- **NP = Section 4.2.3**

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.

- **ST =**
  - Endpoint Management Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard

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.

- **NP = Section 4.4.2**

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.

- **ST =**
  - Endpoint Management Standard
  - Information Technology Inventory Management Standard (future)

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.

- **ST =** Endpoint Management Standard

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.

- **NP = Section 4.2.3**
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.

- Removed, inconsistent with existing Policy at other institutions

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

- Removed, inconsistent with existing Policy at other institutions

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.

  - **ST** = Endpoint Management Standard

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.

  - **ST** = Shared/Cloud File Storage Standard (future)

Server storage should not be used to backup personal documents or data files, such as personal photos, music, or video.

  - **NP** = Section 4.7.1

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.

  - **ST** = Shared/Cloud File Storage Standard (future)

4.4 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.

  - **NP** = Section 4.2.2


  - **Removed, no longer relevant because AUP is at the USNH level**
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.

- **NP** = Section 4.5

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.

- **NP** = Section 5

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.

- **NP** = Section 4.4.2 and 4.4.3.2

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.

- **Removed, inconsistent with existing Policy at other institutions**

4.5 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

- 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.

- **NP** = Section 4.4.3.2, 4.5, 4.10, 5

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.

- **NP** = Section 4.9

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.

- **NP** = Section 4.10

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.

- **NP** = Section 4.10

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.

- **NP** = Section 5

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.

- **NP** = Section 5
4.6 Conduct. Conduct which violates this policy includes, but is not limited to the activities in the following list:

**Unauthorized use of a computer account.**

- NP = Section 4.4.3.1.1

**Using or attempting to use the account of another user.**

- NP = Section 4.4.3.1.2

**Sharing or distributing account passwords, including your own password.**

- NP = Section 4.4.3.1.3

**Using the GSC/University System of New Hampshire network to gain unauthorized access to any computer systems.**

- NP = Section 4.4.3.2.1 and 4.4.3.4.2

**Connecting unauthorized equipment to the GSC/University System of New Hampshire network.**

- NP = Section 4.8

**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.**

- NP = Section 4.4.3.4.3

**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.**

- NP = Section 4.4.3.6

**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.**

- NP = Section 4.4.3.2
Using GSC/University System of New Hampshire resources for commercial activity such as creating products or services for sale.

- **NP** = Section 4.4.3.3

Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.

- **NP** = Section 4.4.3.2.2

Initiating or propagating electronic chain letters.

Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming".

- **NP** = Section 4.4.3.6.1

Forging the identity of a user or machine in an electronic communication.

- **NP** = Section 4.4.3.5

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.

- **NP** = Section 4.4.3.2

Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.

- **NP** = Section 4.4.3.3.5

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.

- **NP** = Section 4.4.3.1

**KSC CNUP**

Current Policy: [https://www.keene.edu/administration/policy/detail/cnup/](https://www.keene.edu/administration/policy/detail/cnup/)

**Summary**

The Information Technology Group (IT Group) has developed the Computer and Network Use Policy (CNUP). This policy is designed to guide individuals in the acceptable use of computers, information systems, and networks owned by Keene State College. More importantly, it is meant as an application of best practices to ensure availability, integrity, reliability, privacy, and confidentiality of college owned computers, information systems, and networks. Keene State College makes computing and network
resources available to faculty, staff, students, and the general public to support the educational, scholarship, research, and service mission of the college.

- **NP** = Section 1, Section 2, and 4.1.2

**Scope**

The Computer and Network Use Policy establishes policy for the use of Keene State College IT and network resources by authorized individuals. It is not designed to cover any situations and circumstances beyond this scope. CNUP supplements other more specifically targeted USNH and KSC policies. The function of this policy is to supplement other USNH and KSC policies and procedures. In cases where multiple policies and/or laws apply these other documents take precedence over CNUP and CNUP will supplement and support them. IT resource owners have the authority to manage their resources to best fit their needs and have the right to establish more restrictive policies and procedures governing their use.

- **NP** = Section 2

**User Responsibilities**

The computing and network resources and services owned by Keene State College are limited and should be used wisely and carefully with consideration for the needs of others.

- **NP** = 4.1.1, 4.2.2

By using computers, information systems, and networks owned by Keene State College, you assume personal responsibility for acceptable use and agree to comply with this policy, other applicable KSC and USNH policies, as well as applicable federal, state, and local laws and regulations.

- **NP** = Section 3

Failure to uphold CNUP acceptable uses constitutes a violation of this policy and may be subject to disciplinary procedures applicable to students, staff, and faculty.

- **NP** = Section 5

**Acceptable Uses**

All users may...

- **NP** = 4.3

Use computing or network resources to support the educational, scholarship, research, and service mission of the college.

- **NP** = 4.3.3.1

Use computing or network resources for personal computing in compliance with this policy.

- **NP** = 4.7
Use only approved computing devices when connecting to the KSC network.

- **NP = 4.8**

The following unacceptable uses apply to all uses of KSC technology resources. In the constantly changing world of information technology, it is impossible to enumerate all non-acceptable uses of KSC computers, information systems, and networks. All users are expected to conduct themselves within acceptable use boundaries and may not infringe on the following examples of unacceptable use.

Unacceptable Uses

All users may not...

- **NP = 4.4**

Use IT resources without proper authorization

- **NP = 4.4.3.1.1**

Attempt to monitor, intercept, analyze or modify network traffic or transactions not specifically addressed to your computer

- **NP = 4.4.3.6.1**

Harass, defame, intimidate or threaten anyone through the use of computing or network resources for sexual harassment issues, see KSC Discrimination & Discriminatory Harassment or the USNH Complaint & Grievance Policy.

- **NP = 4.4.3.2.1 and 4.4.3.2.2**

Use computing or network resources for profit, commercial use or for the purpose of lobbying that connotes College involvement or endorsement of any political candidate or ballot initiative

- **NP = 4.4.3.2.2 and 4.4.3.3.3**

Attempt to alter or reconfigure any KSC IT resources, e.g. network infrastructure, servers

- **NP = 4.4.3.3.4**

Attempt to obtain privileges for which you are not authorized

- **NP = 4.4.3.1.1**

Attempt to access, modify and/or delete another user’s files, configuration or software without the expressed agreement of the owner

- **NP = 4.4.3.1.1**

Attempt to learn another user’s password(s) or personal information

- **NP = 4.4.3.1.2**
Attempt to alter or obscure your identity or your computer’s identity, including but not limited to IP Address and email address, while communicating on any network

- **NP = 4.4.3.5.1**

Interfere with or disrupt computer or network accounts, services or equipment of others including but not limited to consumption of excessive IT resources, (e.g. local area network or Internet bandwidth) through the propagation of worms or viruses or the inappropriate sending of broadcast messages to large number of hosts

- **NP = 4.4.3.4 and 4.4.3.6**

Interfere with or circumvent the IT Group’s responsibilities and procedures

- **NP = 4.4.3.4 and 4.4.3.6**

Consume excessive IT resources, e.g. Local Area Network or Internet Bandwidth

- **NP = 4.4.3.6.1**

Abuse email privileges - see email policy

- **NP = 4.4.3.6.1**

Download and/or share copyrighted material for which you do not have the proper authorization

- **NP = 4.4.3.2.3**

Use unauthorized computing devices when connecting to the KSC network

- **NP = 4.8.3**

Federal, State and Local Laws

All computer and network users are bound by federal, state, and local laws relating to harassment, copyright, security, and privacy relating to digital media. The IT Group will cooperate fully, upon the advice of college legal counsel, with any local, state or federal officials investigating an alleged crime committed by an individual using Keene State College information technology resources. (more...)

- **NP = 4.4.3.2.1**

Policy Enforcement

IT Group system administrators or network administrators may be required to investigate violations of this policy in order to ensure compliance. The IT Group may restrict the use of computers and networks when faced with evidence of violation of this policy or federal, state, or local laws. The IT Group is sensitive to these issues and will remain professional and conscientious while evaluating potential violations. When violations do occur, the IT Group follows the CNUP violation process.

- **NP = 4.10 and Section 5**
IT Group Responsibilities

Beyond controlling access and protecting against unauthorized access and computer or network threats, the IT Group plays a proactive role in implementing and enforcing security or network procedures by following higher education best practices. Using hardware infrastructure and software tools, utilities and applications, the IT Group will maintain a network and computing environment enabling authorized campus users secure, reliable access to internal and external networking resources and applications.

• **NP** = Section 7

Shared and limited technology resources often require prioritization, the IT Group will assign these priorities while managing the network:

**Highest**: Applications and services directly associated with the college mission. Applications and services supporting the college’s business functions.

**Medium**: Non-academic residential personal computing.

**Lowest**: Personal activity, not related to college business, academic and research functions.

• **ST** = Network Security Standard

The IT Group will respect and strive to ensure users’ privacy and intellectual property while managing the computing and network infrastructure and information application transactions and data. The IT Group does not actively monitor network traffic or view content. However, while researching computing and/or network issues, system administrators or network administrators may need to use tools or utilities that expose content or users’ internet habits. Under these circumstances, the IT Group will hold this information and knowledge in strictest confidence.

• **NP** = Section 4.5

The IT Group will not intentionally release or expose a user’s personal information, e.g. name, SSN, Date of birth, etc. to anyone external to KSC or to unauthorized KSC employees. There are many laws and regulations concerning this issue. (more.....)

• **NP** = Section 4.5

At times the IT Group may need to reconfigure network and/or computing resources to mitigate situations that negatively impact access to IT resources. These actions include, but are not limited to, temporarily disabling access to an individual system, temporarily disabling access to/from a specific segment of the LAN or modifying priorities. Though rare and short in duration, these steps are necessary to isolate problems and enable a quick resolution.

• **NP** = Section 5

To report a CNUP violation and/or suspected CNUP violations, contact the Security Manager.
PSU – ACCEPTABLE USE POLICY MAPPING


I. Purpose of the policy

Computing resources ("Resources") at Plymouth State University ("PSU") support the educational, instructional, research, and administrative activities of PSU, and the use of these resources is a privilege extended to members of the PSU Community. Through the privilege to use Resources, a member of the community may have access to valuable PSU tools, services, and sensitive data. Consequently it is imperative to behave in a responsible, reasonable, ethical, and legal manner.

The Acceptable Use Policy ("AUP") seeks to ensure that all members of the PSU Community have appropriate access to functional, safe, and timely computing resources. The AUP seeks to prevent any misuse, damage, inappropriate access to, or illegal use of PSU computing resources.

II. Applicability and Authority

The Acceptable Use Policy applies to all users of computing resources owned, managed, licensed, or entrusted to PSU, regardless of whether the user is on campus or operating from a remote location. Individuals covered by the AUP include, but are not limited to, PSU Faculty, visiting Faculty, Students, Alumni, Staff, guests, agents of the administration, external individuals, and organizations that access PSU computing resources.

Computing resources include, but are not limited to, all PSU owned, licensed, or managed hardware and software, the PSU telephony system, and the use of the PSU wireless and wired data network regardless of the ownership of the device connected to it. Computing resources also include any and all information...
maintained in any form, and in any medium, within the university's physical computing resources or by license on other systems.

- **NP** = Section 8

The AUP applies to all PSU owned and/or licensed computing resources, regardless of the department or individual administering, maintaining it, or scheduling its use.

- **NP** = Section 2

### III. Detailed Policy Statement

PSU has provided access and use of PSU computing resources to members of the PSU Community with a reasonable expectation of unobstructed use, however in turn each member of the PSU Community is responsible for exercising good judgment and knowing and following the regulations and policies of PSU which apply to their use.

- **NP** = 4.1.1, 4.2.1

Just because an action is technically possible does not mean that the action is appropriate and permitted. Members of the PSU Community must comply with Federal, State and local laws; University and University System rules, regulations and policies; and the terms of applicable contracts – including software licenses – when using PSU computing resources.

- **NP** = 4.2.2 and 4.4.2

Plymouth State University reserves the right to access and affect computing resources to the extent necessary to manage and administer the resources. This includes direct access of data on PSU’s networks, PSU owned computing resources, and data stored in PSU systems.

- **NP** = 4.5.5

Acceptable Use is always ethical, reflects academic integrity, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security, and freedom from intimidation and harassment.

- **NP** = 4.3.1, 4.3.2

**Guidelines for Acceptable Behavior:**

Use only computing resources for which you have been granted proper authorization. Access does not imply authorization.

- **NP** = 4.3.3.2

Do not use computing resources to violate any policy or regulation of PSU, the University System of New Hampshire (“USNH”), or federal state or local law

- **NP** = 4.4.2 and 4.4.3.2
Respect the privacy and property of others.

- **NP** = 4.2.2 and 4.5

Employ appropriate standards of civility when communicating with other individuals.

- **NP** = 4.2

Be sensitive to the needs of others, and use only your fair share of computing resources.

- **NP** = 4.3.1

Wired and wireless network services may not be modified or tampered with, nor may they be extended beyond the limits provided.

- **NP** = 4.8.2

You are ultimately responsible for the use of your credentials (“Credentials”) and network connection. This includes your account, computer, network address/port, software and hardware.

- **NP** = 4.4.3.1

You must make a reasonable effort to protect your passwords and secure computing resources against unauthorized use or access.

- **NP** = 4.4.3.1

The use of university computing resources is for PSU related work. Persons are not permitted to engage in consulting or other business ventures using PSU computing resources for personal gain or other commercial purposes.

- **NP** = 4.4.3.3

Do not attempt to circumvent any security measure.

- **NP** = 4.4.3.4.3

The following activities are specifically prohibited:

disclosing your password to others;

- **NP** = 4.4.3.1.3

using somebody else’s password to gain access to PSU and USNH Resources;

- **NP** = 4.4.3.1.2

forging messages;

- **NP** = 4.4.3.5

cracking passwords and systems;
• **NP = 4.4.3.4.3**
  
sending harassing or threatening messages;

• **NP = 4.4.3.2.2**

the sending of unauthorized anonymous messages;

• **NP = 4.4.3.5 and 4.4.3.6.1**

misrepresentation of identity;

• **NP = 4.4.3.5**

the sending of bulk unsolicited messages; phishing;

• **NP = 4.4.3.6.1**

entering, without authorization, into any account to use, read, transfer or change the contents in any way;

• **NP = 4.4.3.1.1**

system attacks; denial of services; and other malicious uses of Resources;

• **NP = 4.4.3.4**

altering system software and/or hardware;

• **NP = 4.4.3.3.4 and 4.4.3.4.1**

and using Resources to interfere with the normal operation of computing systems and connected networks.

• **NP = 4.4.3.3.4, 4.4.3.4.1, 4.4.3.4.3, and 4.4.3.6**

IV. Non-compliance

**Plymouth State University considers violation of the AUP to be a serious offense, and may lead to disciplinary action and/or criminal prosecution. In accordance with established PSU practices, policies and procedures, confirmation of unexcused inappropriate use of PSU computing resources may result in termination of access, expulsion from the University, termination of employment, legal action, and/or other disciplinary measures.**

• **NP = Section 5**

**Plymouth State University reserves the right to take actions to investigate and examine potential violations of the AUP, and to protect computing resources from systems and events that threaten or impact operations. Plymouth State University reserves the right to access, monitor, and report the contents and activity to the proper authorities.**
V. Definitions

PSU Plymouth State University Resources Computing and telecommunications equipment (including computers, tablets and cellphones), software and services maintained or contracted by Plymouth State University or the University System of New Hampshire.

AUP Acceptable Use Policy

USNH University System of New Hampshire

Credentials Username, passwords, PIN numbers, copy codes and access codes

VI. Related Policies / References for More Information

Written Information Security Protocol ("WISP")

UNH - ACCEPTABLE USE FOR INFORMATION TECHNOLOGY RESOURCES


5.1 Introduction. Information technology (IT), the large and growing array of computing and electronic data communications resources, is an integral part of the fulfillment of the University of New Hampshire’s teaching, research, administrative, and service roles. Members of the University community have access to these IT resources and attendant responsibilities not to misuse them. This Acceptable Use Policy (AUP) provides guidelines for the acceptable use of the University's IT resources as well as for the University's access to information to manage these resources.

• NP = Section 1

5.1.2 Use of information technology resources can be broadly categorized as acceptable, allowable, or prohibited.

• Removed, unnecessary excess language, adopted simpler approach taken in other institution’s existing policies
5.1.3 Acceptable use of information technology resources is legal use consistent with the mission of the University of New Hampshire, i.e., use that furthers the University's mission of learning and teaching, research, and outreach.

- **NP = 4.1.1 and 4.3.3.1**

5.1.4 Allowable use is legal use for other purposes that do not impinge on acceptable use. The amount of allowable use will vary over time based on the capacity reserve of information technology resources available beyond Acceptable use.

- Removed, unnecessary excess language, adopted simpler approach taken in other institution’s existing policies

5.1.5 Prohibited use is illegal use and all other use that is neither acceptable nor allowable.

- **NP = 4.4.1**

5.1.6 Most IT use parallels familiar activity in other media and formats, making existing University policies important in determining what use is appropriate. Using electronic mail ("e-mail") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. University policies that already govern freedom of expression, discriminatory harassment, and related matters in the context of standard written expression, govern electronic expression as well. This AUP addresses circumstances that are particular to the IT arena and is intended to augment, but not to supersede, other relevant University policies.

- **NP = 4.1.3**

5.1.7 For statements of other applicable University policies consult the University System of New Hampshire Policy Manual (OLPM); the Financial and Administrative Procedures Manual (FAP); the handbooks for faculty, PAT staff, and operating staff; the Student Rights, Rules, and Responsibilities; and policies that govern use of particular IT systems and labs.

- Removed, unnecessary excess language, adopted simpler approach taken in other institution’s existing policies

See, too, the links to online documents in the Policy Cross-references section below.

- **NP = Section 9**

5.2 Purpose. The purpose of this AUP is to ensure an information technology infrastructure that promotes the basic missions of the University in teaching, research, administration, and service. In particular, this AUP aims to promote these goals:

5.2.1 To ensure the integrity, reliability, availability, and performance of IT resources.

5.2.2 To ensure that use of IT resources is consistent with the principles and values that govern use of other University facilities and services.

5.2.3 To ensure that IT resources are used for their intended purposes.
5.2.4 To establish processes for addressing policy violations and sanctions for those committing violations.

- **NP =** Section 1

5.3 **Definitions**

5.3.1 **OLPM.** "OLPM" is the University System of New Hampshire On-line Policy Manual, which is the master compilation of formal System-wide and Campus-wide institutional policies.

5.3.2 **FAP.** "FAP" refers to the Financial and Administrative Procedures Manual that applies to all the USNH Campuses, as approved by the Board of Trustees or the Financial Policies and Planning Council.

5.3.3 **AUP.** "AUP" is the Acceptable Use Policy for Information Technology resources and refers to this document.

5.3.4 **University.** The term "University" means the University of New Hampshire (UNH), both the Durham and Manchester Campuses.

5.3.5 **IT Resources.** Following the definition in the OLPM (USY.VI.F.4.2), "technological resources shall include, but not be limited to, telephones, voice mail applications, desktop computers, computer networks and electronic mail applications, which are owned or operated by UNH. The term shall also include non-institutional technological resources used in the performance of official duties by faculty, staff, or administrators, but only to the extent of such use."

5.3.6 **User.** A "user" is any person, whether authorized or not, who makes any use of any IT resource from any location. For example, users include those who access IT resources in a University computer lab, or via a electronic network. A "user's status" means their relationship with the University, i.e., student, faculty, staff, contractor, alumni/alumnae, member of public, etc.

5.3.7 **Disciplinary Authority.** If informal resolution does not work or the misuse is more serious, referral is made to the existing University judicial or disciplinary process, as appropriate for the status of the user. For example, students are covered by the Student Code of Conduct and Judicial Process, staff is covered by the OLPM, and faculty is covered by the collective bargaining agreement. This may include University police when the law appears to be broken.

5.3.8 **Systems Authority.** While the University as an entity is the legal owner or operator of all its IT Resources, it delegates oversight of particular systems to the head of a specific subdivision, department, or office of the University ("systems authority"), or to an individual faculty member, in the case of IT resources purchased with research or other funds for which they are individually responsible. For example, the systems authority for the centrally managed Exchange environment is the Assistant Vice President, Enterprise Technology Services.

5.3.9 **System Administrator.** Systems authorities may designate another person as a "system administrator" to manage the particular system resources for which the system authority is
responsible. Systems administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources, in accordance with existing policies and procedures.

5.3.10 Computer account. A "computer account" is any access name and its associated password that is assigned to a user for access to information technology resources.

5.3.11 Specific authorization. This means documented permission provided by the applicable system administrator.

- **NP** = Section 8

5.4 Scope

5.4.1 This Policy applies to all users of IT resources, including but not limited to University students, faculty, and staff, and to the use of all IT resources. These include systems, networks, and facilities administered by UNH Information Technology (UNH IT), as well as those administered by individual schools, departments, University laboratories, and other University-based entities. This includes the general public.

5.4.2 Use of University IT resources, even when carried out on a privately owned computer that is not managed or maintained by the University, is governed by this policy.

- **NP** = Section 2 and Section 3

5.5 Acceptable Use of IT Resources. Although this policy sets forth the general boundaries of acceptable use of IT resources, students, faculty, and staff should consult their respective governing policy manuals for more detailed statements on permitted and appropriate use. This includes the University System of New Hampshire Policy Manual (OLPM); the Financial and Administrative Procedures Manual (FAP); the handbooks for faculty, PAT staff, and operating staff; the Student Rights, Rules, and Responsibilities; and specific restrictions that system administrators may place on resource use.

- Removed, unnecessary excess language, adopted simpler approach taken in other institution’s existing policies, intent is addressed in section 5 and section 9

IT resource authorities or administrators may elect to impose stricter controls than those required by this policy. In all cases where the controls are less restrictive than those of this AUP, this AUP applies.

- **NP** = Section 2

5.5.1 IT resources may be used only for their authorized purposes, that is, to support the University’s primary mission of teaching, research, and outreach (BOT.II.H.1.1). The particular purposes of any IT resources, as well as the nature and scope of authorized use and incidental personal use, may vary according to the duties and responsibilities of the user.

- **NP** = 4.3.3.2, 4.7
5.5.2 Proper authorization. Users are entitled to access only those elements of IT Resources that are consistent with their authorization.

- **NP = 4.3.3.2**

5.5.3 Allowable use. Incidental personal use of IT resources is allowed, such as Web browsing and personal e-mail, as long as it is consistent with this AUP and any applicable departmental work-unit policies and guidelines. The capacity of IT resources available beyond acceptable use will vary over time and so individual use will be restricted if it interferes with the University's primary mission.

- **NP = 4.7**

5.6 Prohibited Use. Prohibited use is illegal use and all other use that is neither acceptable nor allowable. The following categories of use are inappropriate and prohibited.

- **NP = 4.4**

5.6.1 Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not interfere with, or attempt to interfere with, the normal use of IT resources by other users. Interference includes: denial of service attacks, misusing mailing lists, propagating chain letters or hoaxes, and intentional or unintentional sending of unwanted e-mail to users without specific authorization or a way to opt-out (“slamming”).

- **NP = 4.4.3.6.1**

Other behaviors that cause a network traffic load or computing load that interferes with the normal and intended use of the IT resources is also prohibited.

- **NP = 4.4.1**

5.6.2 Use that is inconsistent with the University's non-profit status. The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters.

- **NP = 4.4.3.3.1**

As a result, commercial use of IT resources for non-University purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies (FAP 8-006).

- **NP = 4.4.3.3.2**

System administrators are expected to develop more detailed guidance for the use of e-mail, Web pages, and other services on specific IT resources.

- Removed, inconsistent with existing policies at other institutions, intent addressed by development of related Standards which will provide detailed guidance for use of specific resources
5.6.3 Use of IT resources in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT resources for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with the University System of New Hampshire General Counsel’s Office.

- NP = 4.4.3.3.3

5.6.4 Harassing or threatening use. This category includes, for example, discriminatory harassment, display of offensive or sexual material in the workplace, and repeated unwelcome contacts with another.

- NP = 4.4.3.2 and 4.4.3.3.5

5.6.5 Use that damages the integrity of University or other IT resources. This category includes, but is not limited to, the following activities:

- NP = 4.4.3.4

5.6.5.1 Attempts to defeat system security. Users must not defeat or attempt to defeat any IT resources security, such as by analysis ("cracking") or guessing and applying the password of another user, or by compromising room locks or alarm systems. This provision does not prohibit, however, UNH IT or system administrators from using security-scanning programs within the scope of their systems authority.

- NP = 4.4.3.4.3

5.6.5.2 Unauthorized access or use. The University recognizes the importance of preserving the privacy of users and data stored in IT systems. Users must honor this principle by refraining from, or assisting, unauthorized access to IT resources. This applies to a variety of situations:

- NP = 4.4.3.1.1

5.6.5.2.1 For example, a non-University organization or individual may not use non-public IT resources without specific authorization.

- NP = 4.4.3.1.4

5.6.5.2.2 For example, privately owned computers may be used to provide public information resources, but such computers may not host sites or services, across the University network, for non-University organizations without specific authorization.

- NP = 4.6.3

5.6.5.2.3 For example, users are prohibited from accessing or attempting to access data on IT resources that they are not authorized to access.

- NP = 4.4.3.1.1
5.6.5.2.4 For example, users must not make or attempt to make any deliberate, unauthorized changes to data on an IT system.

- NP = 4.4.3.3.4

5.6.5.3 Networking equipment and software. Unless specifically authorized, by the network system administrator no user will connect networking equipment (routers, hubs, "sniffers," etc.) to the campus network, nor operate network services software (routing, "sniffing," name service, multicast services, etc.) on a computer attached to the network.

- NP = 4.8.1

5.6.5.4 Disguised use: Users must not conceal their identity when using IT resources, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

- NP = 4.4.3.5

5.6.5.5 Distributing computer hoaxes and viruses. Users must not knowingly distribute or launch hoaxes, computer viruses, worms, or other rogue programs intended to compromise IT resources.

- NP = 4.4.3.6.1 and 4.4.3.6.3

5.6.5.6 Removal of data or equipment. Without specific authorization by a system administrator, users must not remove any University-owned or administered IT resource equipment from its normal location.

- NP = 4.4.3.6.2

5.6.6 Violation of law

5.6.6.1 Illegal use of IT resources, i.e., use in violation of civil or criminal law at the federal, state, or local levels is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

- NP = 4.4.3.2

5.6.6.2 With respect to copyright infringement, users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for limited "fair use". Educational use must meet the normal fair use guidelines.

- NP = 4.3.3.3 and 4.4.3.2.3
5.6.7 Violation of University contracts. All use of IT resources must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.

- NP = 4.4.2

5.6.8 Violation of external data network policies. Users must observe all applicable policies of external data networks when using such networks.

- NP = 4.4.3.4.2

5.7 Personal Account Responsibility. Users are responsible for maintaining the security of their own accounts and passwords for access to IT resources. Accounts and passwords are normally assigned to individual users and are not to be shared with any other person without authorization by the applicable system administrator. Users are presumed to be responsible for any activity carried out under their IT system accounts or posted on their personal Web pages.

- NP = 4.2.2, 4.4.3.1.2, 4.4.3.1.3

5.8 Personal Identification. Upon request by a system administrator or other University authority, users must produce valid identification.

- Removed, inconsistent with existing policies at other institutions, cannot practically be enforced/implemented, intent covered in identity verification requirements included in Identity Management Standard, Access Management Standard, and Account Management Standard

5.9 Conditions of University Access to Resources. There 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.

- NP = 4.5 and 4.9
- ST = Access to Password Protected Information Standard

5.9.1 Special Conditions. The following special conditions for institutional access to IT materials, without the consent of the user, would operate under the procedural safeguards specified in UNH.VI.F.4.4.

5.9.2 Diagnosis. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT resources.

5.9.3 Required by law. When required by federal, state, or local law or administrative rules.

5.9.4 Reasonable grounds. When there are reasonable grounds to believe that a violation of law may have taken place and access and inspection or monitoring may produce evidence related to the violation.
5.9.5 Essential business. When such access to IT resources is required to carry out essential business functions of the University.

5.9.6 Health and safety. When required to preserve public health and safety.

  - NP = 4.5
  - ST = Access to Password Protected Information Standard

5.10 Process. Consistent with the procedures specified in the OLPM for institutional access to materials and records without the consent of the user, such access is to be logged by the system administrator for subsequent review by the appropriate Vice President (UNH.VI.F.4.4).

  - NP = 4.5
  - ST = Access to Password Protected Information Standard

5.10.1 User access deactivation. The University, through the appropriate system administrator, may deactivate a user’s information technology privileges, even in the absence of a suspected AUP violation, when necessary to preserve the integrity of IT resources. The system administrator must notify the user in writing of any such action within 48 hours (UNH.VI.F.4.4).

  - NP = 4.9, some requirements removed as they are inconsistent with other institution’s policies and not practically enforceable

5.10.2 Security scanning systems. By attaching privately owned personal computers or other IT resources to the University’s network, users consent to the University use of security scanning programs while connected to the network.

  - NP = 4.6.2.1

5.10.3 Logs. Most IT systems routinely log user actions for a variety of reasons, including system recovery, trouble-shooting, usage reporting, and resource planning. All system administrators are expected to establish and post a description of the logging policies and procedures for the systems they manage. This may take the form of a privacy statement or a more general operational statement.

  - Removed, inconsistent with existing policies at other institutions

5.10.4 Encrypted material. University faculty and staff, as employees, may encrypt files, documents, and messages for protection against unauthorized disclosure while in storage or in transit. However, such encryption must allow officials, when properly required and authorized, to decrypt the information (UNH.VI.F.4).

  - Removed, inconsistent with existing policies at other institutions

5.11 Enforcement Procedures

- NP = Section 5
5.11.1 Complaints of Alleged Violations. An important element in the enforcement of violations of this AUP is the intent, i.e., whether a violation was carried out with knowledge and awareness of the consequences. For minor violations the expectation is to resolve the violation at the lowest level of system administration involved. System administrators are expected to apply judgment in reporting a violation to a formal judicial or disciplinary process. The AUP administrator may be consulted for interpretive advice, as described below. Seen as a simple diagram:

An individual who believes that they are harmed by an alleged violation of this policy may file a complaint in accordance with established University complaint or grievance procedures. The individual is also encouraged to report the alleged violation to the systems authority responsible and to refer the matter to University disciplinary authorities.

- NP = 4.10

5.11.2 Reporting Observed Violations. If an individual has observed or otherwise is aware of an alleged violation of the AUP, but has not been harmed by the alleged violation, they may report the matter to the systems authority responsible for the facility most directly involved and refer the matter to University disciplinary authorities.

- NP = 4.10

5.11.3 Disciplinary Procedures. When possible, the goal is to resolve issues of use and misuse informally between the user and relevant system administrator, including use of informal departmental procedures if helpful.

Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for students, faculty, and staff, as outlined in the relevant student regulations (e.g., Student Rights, Rules, and Responsibilities), the faculty handbook, or staff handbook. Faculty or staff who are members of University-recognized bargaining units are covered by disciplinary provisions set forth in the agreement for their bargaining units. Factors to consider in an alleged incident are: its nature, the intent, extent of damage, and history of offenses, leading to a recommended action.

Systems administrators may participate in formal disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. And, at the direction of the appropriate disciplinary authority, systems administrators are authorized to investigate alleged violations.

- NP = Section 5

5.11.4 Penalties. Users found to have violated this AUP are subject to penalties provided for in other University policies dealing with the underlying conduct. Such users may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the system administrator.

System administrators in violation of their authority are also subject to penalties as provided in other University policies.
5.11.5 Legal Liability for Unlawful Use. In addition to University discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT resources.

5.11.6 Appeals. Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the formal appeals provisions of the relevant disciplinary authority.

5.12 Policy Development

5.12.1 This AUP will be periodically reviewed and modified under the direction of the Assistant Vice President for Computing and Information Services, in consultation with University committees and constituencies. This Assistant Vice President will designate an AUP administrator to assist with:

5.12.1.1 Interpretation. For questions or assistance about the interpretation of this AUP, contact the AUP administrator.

5.12.2 Review. This AUP will be reviewed for accuracy as needed, but not less than once a year, by the AUP administrator.

5.13 Policy Cross-references. The following links are to related online policies and documents. There are other important policies and documents that are not yet online.

5.13.1 Digital Millennium Copyright Act
5.13.2 FAP on Charitable and Political Contributions Procedure 8-006
5.13.3 Library Records Confidentiality
5.13.4 NH RSA 638:16,17,18. State statutes on computer crime
5.13.5 OLPM on Mailing Lists and Directories (UNH.III.B)
5.13.6 OLPM on Privacy and Security of Technological Resources (UNH.VI.F.4)
5.13.7 Student Rights, Rules, and Responsibilities. See Appendix for the Family Educational Rights and Privacy Act of 1974 (FERPA), a/k/a "The Buckley Amendment."
5.13.8 UNH Primer on Copyright Law and Recommended Procedures
5.13.9 UNHINFO Privacy Statement
This AUP was modeled, with permission, on the appropriate use policy at Yale University and conforms to UNH.III.E for institutional policy development, review, and approval.