University of Vermont

OFFICE OF COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

FOR PRINTED USE ONLY

Policies residing on UVM's Institutional Policy website are the most current versions available. If you are viewing a policy anywhere else including in printed form or embedded on other websites, it may not be the most current.

Title: Computer, Communication, and Network Technology Acceptable Use

Policy Statement

By accepting or using any UVM computer, network account or connection, or other information and communication technology services provided to him or her by the University, each User understands and agrees to the following (click on link for elaboration):

1. **Account Responsibility:** Individual Users are responsible for all uses of University-provided computers, network connections and accounts, and other information and communication technology services, including data backup and password maintenance, under the electronic identity assigned to them by the University.

2. **Information Security**: Each User who generates, collects, stores, uses, processes, administers, or maintains information to conduct University business is responsible for its appropriate use and its protection. The University will document standard practices that are required of all individuals who have those responsibilities.

3. **Account Security and Information Privacy**: The University strives to maintain the security of personal accounts, but Users should not presume that information in network-based file repositories or on University-owned or -administered computers and servers is private.

4. **Prohibited Uses:** Uses that are illegal, that are contrary to UVM policy, or that interfere with system or network performance or with other legitimate uses are prohibited.

5. **Responsibility for Information:** The University does not monitor and is not responsible for the contents of the accounts and other information and communication technology services it provides. Each User is responsible for all information they access, make available, or distribute.

6. **Personal Use of Resources:** Users may use their computers, network accounts, and other information and communication technology services provided to them by the University for occasional and incidental non-University matters, except as otherwise prohibited by this or other University policy or when the use unreasonably interferes with academic uses, job performance, or system performance or operations. Personal use is subject to the terms of this Policy, including those terms regarding access to information on University computers and accounts.

7. **No Personal Financial Gain:** Users agree not to use computers, network connections and accounts, or other information and communication technology services for the operation of private enterprises or for private fund-raising.

8. **Enforcement:** Users understand that violations of this Policy may result in suspension or termination of access to UVM's network or to services available through that network and may result in disciplinary action including academic expulsion, employment termination, or criminal prosecution.

9. **Administrative Interpretation:** By accepting an electronic identity or using the University's resources or services, Users agree to read and abide by this Policy and its administrative interpretations as they may be amended from time to time.

Reason for the Policy

The University of Vermont provides a wide array of computing, communication, networking, and other information technology resources to students, staff, and faculty to advance the educational, research, and land-grant missions of the institution. Those resources are critical to the University's continued operation and to the success of our community members in their learning, teaching, scholarship, and service. This Policy sets forth the University's expectations for the acceptable use of those resources.

Applicability of the Policy

This Policy applies to all University of Vermont faculty, staff, students, and other individuals who use computers, network accounts, the University e-mail system, or other information and communication technology services or resources ("Users"). The Policy applies whether UVM information technology resources are accessed remotely or through the use of a University-owned device or UVM network connection.

Definitions

Broadcast: Transmission of a message to the University community at large, or major populations thereof (such as all students, faculty, or staff), through a University server or servers.

Electronic communication: Any electronic method or system used to communicate between or among individuals or groups, or to post information, including, but not limited to, email and internet forums, such as social media platforms, websites, blogs, and wikis.

Information and communication technology services or resources: Includes information in any form and recorded on any media, and all computer and communication resources such as equipment, storage devices and media, information in transit, and software. Includes all information that the University or its agents use in the course of conducting University business, except those materials specifically excluded from University ownership as set forth in the University's Intellectual Property Policy.

Users: All University of Vermont faculty, staff, students, and other individuals who use University computers, network connectivity, network accounts, the University e-mail system, or other UVM-owned or administered information and communication technology services or resources.

Procedures

Details regarding ETS policies, procedures, and practices that implement this Policy are available at the ETS "Information Policy and Security Operating Procedures" web site (https://www.uvm.edu/it/it-policies).

Elaboration

NOTE: Each numbered Policy section is followed by an Administrative Interpretation that provides additional guidance as to the meaning of the Policy. It does not limit the plain meaning of the terms of the Policy, but, rather, seeks to provide additional information and further explain University requirements and expectations.

1. **Account Responsibility**

   Individual Users are responsible for all uses of University-provided computers, network connections and accounts, and other information and communication technology services, including local data backup and password maintenance, under the electronic identity assigned to them by the University.

   a. University-provided computers and network accounts may only be used by the individual to whom they are assigned unless otherwise authorized by the University. Access to computers and network accounts for maintenance or service purposes by persons responsible for departmental computing support and Enterprise Technology Services ("ETS") is considered authorized.

   b. Responsible use includes choosing passwords that are not easily deduced by others. The University has implemented strong password management techniques to help ensure password security by requiring minimum password "strength" and routine changes of passwords.

   c. Voluntary unauthorized disclosure of a password may result in suspension, revocation, or denial of computing privileges. Technology support staff will not ask for passwords, nor should passwords be provided to them. If it is necessary to share a password with support staff, the password should be changed immediately after the work has been completed.

   d. Users who suspect that their University-provided computers or network accounts have been accessed without their permission must change their passwords immediately and report the suspected activity to the Information Security Office (iso@list.uvm.edu).

2. **Information Security**
   Each User who generates, collects, stores, uses, processes, administers, or maintains information to conduct University business is responsible for its appropriate use and its protection. The University will document standard practices that are required of all individuals who have those responsibilities.

3. **Account Security and Information Privacy**

   The University strives to maintain the security of personal accounts, but Users should not presume that information in network-based file repositories or on University-owned or administered computers or servers is private.

   a. Files stored in personal (home) directories are normally managed by the User, who may create or delete files or grant access to files to others. Files stored in departmental file stores are normally managed by departmental faculty and staff under the direction of department managers. Department managers may gain access to or have access granted to documents or email stored in faculty and staff home directories subject to formal approval (3.f.i).

b. Business documents are most appropriately housed in departmental directories on institutionally-supported file servers. When an employee leaves UVM, the employee's manager is responsible for recovering University documents that are stored in personal directories or on local storage devices.

c. The University cannot and does not guarantee the confidentiality of electronic information. In addition to accidental and intentional breaches of security, the University may be compelled to disclose electronic information as required by law.

d. As part of its necessary backup and recovery, problem resolution, and security-incident investigation operations, ETS personnel routinely access network accounts and other computing services that the University makes directly or indirectly available to the campus community. Suspected policy or legal violations discovered during such routine operations may be reported to the Chief Information Officer (CIO) or law enforcement officials. Information accessed during routine operations may be released only as permitted by law. Email and other documents stored on University equipment are subject to public records laws and may be requested by and disclosed to members of the public.

e. Unless otherwise prohibited by law, and subject to legal requirements, the University and law enforcement personnel may access computers, network accounts or any other electronic information or technology necessary to investigate suspected unlawful activity or violations of University policy.

f. For accounts granted to University employees, and for University-owned or University-administered computers they use:

   i. With the approval of the Senior Vice President or her/his designee, department heads may obtain access to the computers and the accounts of their subordinates (both current and former employees).
   ii. Department heads may request the suspension or termination of accounts within their departments.
   iii. Department heads are responsible for moving needed files off terminated employees' accounts and off University-owned or administered computers within one month of termination.

4. **Prohibited Uses**

Uses that are illegal, that are contrary to UVM policy, or that interfere with system or network performance or with other legitimate uses are prohibited.

a. Unlawful use of computers or network accounts includes, but is not limited to, defamation; obscenity; unlawful discrimination or harassment; violation of copyrights, trademarks, or licenses; and violation of other rights. Users should be aware that privacy laws in other states and other nations may differ from Vermont's laws, and it may be incumbent upon them to become familiar with those laws before using foreign facilities to support their work.

b. The following acts are also expressly prohibited:

   i. attempts to gain unauthorized access to data or accounts (UVM's or others);
   ii. breach of security measures on any electronic communications system;
   iii. interception of electronic communication transmissions without proper authority;
   iv. unauthorized alteration of software or hardware configurations;
   v. transmission of e-mail messages, or development of other electronic information, that is falsely or inaccurately attributed to another person;
   vi. use of UVM computing or communication resources to harass others or falsify identity;

vii. use of UVM computing or communication resources to disclose confidential information;
viii. use of UVM computing or communication resources to develop or propagate computer viruses, worms, Trojan horses, keystroke loggers, etc.; and
ix. allowing others to use one's University-provided information and communication technology services except as otherwise permitted.

c. Individuals may not "broadcast" e-mail messages without the express advance approval of the Senior Vice President or their designee. This rule does not prohibit University administrators from communicating with their units, nor representatives with their constituencies, nor does it prohibit systems managers from broadcasting messages related to system management and security.

d. University e-mail services shall not be used for purposes that could reasonably be expected to cause undue strain on computing facilities or interfere with others' use of e-mail or e-mail systems. Prohibited uses include but are not limited to: (i) forwarding chain letters; (ii) generating "spam" (exploitation of listservs or similar systems for the widespread distribution of unsolicited e-mail); and (iii) denial of service, for example resending the same e-mail message repeatedly to one or more recipients.

e. Users may not use University information or communication technology services for political campaign activities except as permitted under the Political Activities Policy. All Users must take care to avoid any implication that the University supports or opposes any political candidate, party, or campaign.

f. Properly configured computers and printers may be attached to the UVM network without explicit permission. To safeguard network security and performance, no other device or network service such as routers, hubs, sniffers, or wireless access points may be placed on the network without approval from ETS Telecommunication and Network Services.

5. **Responsibility for Information**

The University does not monitor and is not responsible for the contents of the accounts and other information and communication technology services it provides. Each User is responsible for all information they access, make available, or distribute.

a. Faculty and staff engaged in professional communications are expected to adhere to the same standards of professionalism when using the medium of e-mail, blogging, or other forms of electronic communication as they would when using traditional paper-based media. Use of "embedded messages," quotations, or "taglines" in signatures on communications relating to University business is expressly discouraged insofar as it is inconsistent with those standards or implies University endorsement or sponsorship of personal views. Failure to abide by those standards or to use a required disclaimer may give rise to disciplinary action under applicable disciplinary procedures.

b. Failure to follow legal requirements with regard to the preservation and production of records, including email and calendar information, may lead to disciplinary action as well as civil or criminal charges against culpable individuals. Individuals should review Policy 9.0.3.1, Records Management and Retention Policy, and seek the advice of University legal counsel if they have questions regarding rules applicable to the preservation or production of e-mail records.

6. **Personal Use of Resources**

Users may use their computers, network accounts, and other information and communication technology

services provided to them by the University for occasional and incidental non-University matters, except as otherwise prohibited by this or other University policy or when the use unreasonably interferes with academic uses, job performance, or system performance or operations. Personal use is subject to the terms of this Policy, including those terms regarding access to information on University computers and accounts.

a. Students and employees are strongly encouraged to remove any personal information they may have stored on University-owned computers and network accounts before ending their relationship with the University. Generally, the University will destroy information left on computers and network accounts. Information will be retained if retention is in the University's best interest, and the University will provide prior notice to the student or employee before such retained information is deleted. If the University extends an individual's account access beyond enrollment or employment, stored data will ordinarily be preserved until the extension has ended.

b. E-mail is a communication vehicle primarily intended to serve University programs, activities and operations and thus to promote fulfillment of the institutional mission. Other uses are secondary and permissible only insofar as they do not unreasonably interfere with the primary intended use.

c. The University supports and respects the principles of free expression and the exchange of ideas. However, in the content of electronic communications, users must distinguish personal views from those that they are authorized to express on behalf of the University. When offering personal views in ways that may reasonably be construed as implying the support, endorsement, or opposition of the University, the material shall be accompanied by a disclaimer, such as the following: "The opinions or statements expressed herein are my own and do not represent a position, opinion, or endorsement of the University of Vermont." Guidance as to when a disclaimer is necessary or desirable may be obtained from the Office of the Senior Vice President or the Office of the General Counsel.

d. UVM does not indemnify users of its computing resources for material posted or distributed through electronic communications that may be subject to legal action.

7. **No Personal Financial Gain**

Users agree not to use computers, network connections and accounts, or other information and communication technology services for the operation of private enterprises or for private fund-raising.

a. University personnel may engage in fund-raising and commercial activity on behalf of the University in connection with official University-related duties or University-sanctioned activities.

b. Students residing in campus facilities are permitted to use their workstations on the campus network to advertise personal items for sale on electronic forums in accordance with those sites' terms of service. Other users are permitted to use the campus network, in accordance with Section 6 above, to advertise personal items for sale on electronic forums that allow occasional, casual postings, but the advertisement(s) should not interfere with the intended purposes of those forums or with the academic uses, job performance, or system performance or operations of the campus network.

8. **Enforcement**

Users understand that violations of this Policy may result in suspension or termination of access to UVM's network or to services available through that network and may result in disciplinary action including academic expulsion, employment termination, or criminal prosecution.

a. The University may temporarily suspend a User's computing privileges, network accounts, or other information and communication technology services for security or other administrative reasons. Absent extenuating circumstances, no service may be suspended pursuant to this Policy for more than ten business days unless a disciplinary process has been invoked.

b. Suspected violations by students will be reported to the Student Affairs judicial system. Suspected violations by University employees, whether faculty or staff, will be reported to the employee's supervisor and handled through normal channels established for disciplinary action. For Users not subject to University disciplinary processes, accounts may be summarily suspended or terminated at the discretion of the CIO, and Users may request review of those decisions by the Dean of University Libraries and Chief Information Officer or their designee.

c. Pending resolution of the disciplinary process, the Chief Information Officer (CIO) or designee may suspend University information and communication technology services if the alleged violation is reasonably perceived to constitute unlawful activity, pose a substantial risk to the integrity of University information and communication technology services, or present an imminent threat to the safety or welfare of the campus or members of the University community. In the event of a perceived emergency or if other exigent circumstances demand immediate action, the CIO or designee may immediately suspend information and communication technology services, and notice will be given to the User as soon after as reasonably possible. In non-emergency situations, the CIO or designee will provide the User with notice of the perceived problem and an opportunity to be heard before services are suspended. A suspension may be appealed in writing to the Provost or designee within three business days of the effective date of the suspension. The Provost or designee will provide a written decision to the CIO and the user within five business days of receipt of the appeal. The Provost's or designee's decision will remain in effect pending final resolution of the disciplinary proceeding.

d. Sanctions for violations of this Policy will be imposed by the administrative official with final responsibility for resolution of the disciplinary process in use, following consultation with the CIO if sanctions involve University information and communication technology services. Sanctions with respect to University information and communication technology services may include suspension or permanent revocation of services. If a User who loses their computing privileges cannot perform their job without those services, the User's employment may be suspended or terminated. The University reserves the right to seek restitution or indemnification from a User for expenses arising from violations of this Policy. In addition, the University or third parties may pursue criminal or civil prosecution for violations of law.

e. Users may be subject to discipline under this and other University policies, and users may be subject to laws in other states and nations that govern electronic communications.

9. **Administrative Interpretation**

By accepting an electronic identity or using the University's resources or services, Users agree to read and abide by this Policy and its administrative interpretations as they may be amended from time to time.

a. The Provost is responsible for providing administrative interpretation, which will be modified periodically in light of experience gained and legal and administrative developments.

b. Individuals are responsible for reviewing this Policy and its administrative interpretations on a routine basis.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	**Contact Information:**
Chief Information Officer	234 Waterman Building (802) 656-5598

Forms/Flowcharts/Diagrams

- TBD.

Related Documents/Policies

- Code of Conduct and Ethical Standards
- FERPA Rights Disclosure Policy
- Information Security Policy
- Intellectual Property Policy
- Enterprise Technology Services Policies and Procedures
- Political Activities: Tax Exempt Organization Restrictions
- Solicitation
- Records Management and Retention Policy
- University Sponsored Social Media Guidelines

Regulatory References/Citations

None.

Training/Education

Training will be provided on an as-needed basis as determined by the Approval Authority or the Responsible Official.

About this Policy

Responsible Official:	The Chief Information Officer	**Approval Authority:**	President
Policy Number:	1.8.2	**Effective Date:**	April 12, 2010
Revision History:	Approved by the President on April 12, 2010		