DARTMOUTH

Dartmouth Information Technology Policy

Additional Details

POLICY ID
054-0003

EFFECTIVE DATE
November 7, 2018

DIVISION
Office of the Provost

OFFICE OF PRIMARY RESPONSIBILITY
Information, Technology and Consulting (ITC) (https://itc.dartmouth.edu/)

Summary of Policy

Governs how faculty, students, and staff can use Dartmouth's information technology resources. If a member of the community fails to comply with this policy or relevant laws and contractual obligations, that member's privilege to access and use of Dartmouth's information technology resources may be revoked.

Affected Parties

All Groups

Policy Statement

The Dartmouth College Information Technology Policy (the "Policy") set forth below contains Dartmouth's philosophy and requirements governing student, faculty, staff and alumni use of its information technology resources. Dartmouth College expects each member of the community to use Dartmouth's information technology resources, including connections to resources external to Dartmouth that are made possible by Dartmouth's information technology resources, responsibly, ethically, and in compliance with the Policy, relevant laws, and all contractual obligations to third parties. The use of Dartmouth's information technology resources is a privilege. If a member of the community fails to comply with this Policy or relevant laws and contractual obligations, that member's privilege to access and use Dartmouth's information technology resources may be revoked. The use of Dartmouth's information technology resources to send communications

to Dartmouth or non-Dartmouth persons or entities typically identifies the sender as belonging to the Dartmouth community. Each member of the community should therefore recognize that any such communication may reflect on how Dartmouth is perceived by not only the Dartmouth community, but also the public at large.

By adopting the Policy, Dartmouth recognizes that all Dartmouth students, faculty, staff and alumni who use Dartmouth's information technology resources are bound not only by the Policy, but also by local, state, and federal laws relating to electronic media, copyrights, privacy, and security. Other Dartmouth policies that relate to this Policy and also apply to Dartmouth College students, faculty, staff and alumni (collectively, the "community") include the Dartmouth College Copyright Policy & Guidelines on copyrighted materials, the Dartmouth College Patent Policy, the Dartmouth College student handbooks and faculty handbooks, and the Dartmouth College Exempt and Non-exempt Staff Handbooks. Each member of the Dartmouth community is expected to be familiar with the relevant foregoing policies.

Freedom of Expression

Freedom of expression and an open environment within which to pursue scholarly inquiry and to share information are encouraged, supported, and protected at Dartmouth. (Please see the principle of "Freedom of Expression and Dissent" that appears in the Handbook of the Faculty of Arts and Sciences (https://faculty.dartmouth.edu/dean/sites/faculty_dean.prod/files/dean_faculty/wysiwyg/facultyhandbook_jul_2021_ii.pdf) and the Student Handbook (http://student-affairs.dartmouth.edu/resources/student-handbook/).) Censorship is not compatible with the goals of Dartmouth. While Dartmouth may limit the use of some computers or resources to specific research or teaching missions, freedom of expression will generally be protected. While Dartmouth rejects censorship, behavior that constitutes misconduct will not be protected. Such behavior includes, but is not limited to, the use of Dartmouth's information technology resources in connection with child pornography, harassment of any kind, copyright infringement, theft, unauthorized access, and other violations of the law.

To comply with federal regulations governing tax-exempt organizations, Dartmouth technology resources may not be used for mass and unsolicited communications used in connection with lobbying (except official Dartmouth activities authorized by the Office of the Provost) or political campaigns. Communications that in part may contain political information, when sent to a select few individuals and that pertain to professional and work related issues, are permissible. In addition, such resources should not be used for private business or commercial activities, except where such activities are otherwise permitted under applicable Dartmouth policies.

Privacy

Members of the Dartmouth community have reasonable expectations of privacy in their use of information resources, in accordance with this policy. State and federal law, and Dartmouth policy, prohibits unauthorized access to computer and telephone systems. No one should use aliases, nicknames, pointers, or other electronic means to capture information intended for others without permission of the intended recipient. Attempts to gain unauthorized access to machines or computer records, to decrypt encrypted materials, to monitor other individuals' computer or network use, to attempt to obtain their passwords, or to obtain privileges or information to which the user is not entitled, are prohibited.

Information stored on an individual's account is presumed to be private unless the account holder has made the information available to others. If, for example, the account holder allows public access to files via file sharing, it is presumed that the account holder has waived his or her privacy rights to those files.

Systems operators, supervisors, and other College officials may access information resources to locate business information, maintain the system and network, comply with legal requirements, or administer this or other Dartmouth policies.

Local area networks and local resources, including personal computers, workstations, file servers, printers, and similar devices, shall be subject to the same rights to privacy and confidentiality afforded centralized computer systems, regardless of whether those local resources are connected to any of Dartmouth's central information technology networks.

Some programs and networked services gather information about the people who use them. If such information could directly or indirectly identify a person using the program, then each user should be warned and given a chance to leave the program or service before data collection begins, a procedure referred to as a "privacy warning." To avoid issuing excessive numbers of warning messages, an exception is made for host operating systems and some networked utilities used by Information, Technology & Consulting (ITC) that collect identifying information as part of their normal operation. A list of these exempted programs and services and the data that they collect is available from ITC and is provided in the appendix below. The provider of any program or service that gathers information about those who use it must either install a privacy warning or request ITC to place the program or service on the list of exempted programs.

Intellectual Property

Dartmouth expects all members of the community to be aware of how intellectual property laws, regulations, and policies apply to the electronic environment and to respect the property of others. For more information, please see the Dartmouth College Copyright Policy, the Dartmouth College Policy and Guidelines on Copyrighted Materials, the Dartmouth College Patent Policy, the Dartmouth College Sources manual, the Dartmouth College Academic Honor Principle, the Dartmouth College faculty handbooks, and the Student Handbook. Dartmouth's DMCA Compliance Officer (Digital Millennium Copyright Act) is listed on the Dartmouth Copyright Policy website.

No member of the community shall use another's content or property in a way that violates copyright law or infringes upon the rights held by others. The unauthorized duplication or use of any software that is licensed or protected by copyright may constitute violations of civil and criminal law, and is prohibited by this policy.

Members of the community should recognize that placing their work in the electronic public domain may result in widespread distribution of their work and could jeopardize their rights to that work. You should assume that works communicated through the network are subject to copyright unless there is a specific disclaimer to the contrary.

All computer software used by members of the Dartmouth community must be properly and legally licensed and used. Dartmouth College licenses the use of many different software programs from vendors and developers. In addition, employees and students purchase software with licensing and use agreements. All Dartmouth employees and students are expected to use software in accordance with the appropriate licensing agreements. Failure to do so can result in legal liability, both to Dartmouth and to the individual. The fact that Dartmouth College is an educational institution does not confer rights to copy or use software in any way not authorized by the provisions of licensing and use agreements.

Allocation of Resources

Members of the Dartmouth community are entitled to a fair share of information resources. No one shall attempt to degrade Dartmouth or non-Dartmouth computer systems, networks, or personal computer performance, or to deprive other users, within and without the community, of information resources or authorized access to any College or individually owned computer.

Loopholes in the Dartmouth computer systems and network or knowledge of a special password shall not be used to damage computer systems or networks, to obtain unauthorized resources, or to take resources from other users, either at Dartmouth or elsewhere.

Unauthorized use of College-owned computing resources for commercial purposes is prohibited.

When necessary for the maintenance or mediated allocation of a system

Account and Naming Procedures

The names of students, faculty, staff and alumni are entered into an electronic database of names along with associated items of information. An entry in the Dartmouth name database, administered by Information Technology & Consulting (ITC), grants access to network services that originate at Dartmouth College and that require user authentication, including, for example, Dartmouth's email system and access-restricted information resources. Increasingly, access to the Dartmouth network is determined by whether one has an entry in the central name database and the attributes associated with that entry. Some members of the Dartmouth community are also granted user names and accounts in other name directories on various Dartmouth College computing systems in order to gain authenticated access to and complete work for Dartmouth College. Within this section, an entry in the name database, user name, NetID, other mechanism of authentication and authorization, or account will be referred to as an "account."

Having an account is a privilege, not a right or entitlement. An individual is assigned an account for use while conducting activities related to Dartmouth College. The holder of an account may not share access information that would enable use of an account with anyone, including colleagues at Dartmouth or elsewhere, nor family members. Any and all accounts may be revoked temporarily or permanently if one's information technology related behaviors fall within one or more of the following circumstances:

1. Involvement in criminal activity, regardless of whether such activity is alleged or one is convicted of such activity by a court of law;
2. Behavior that constitutes a violation of a Dartmouth code or policy, including this policy;
3. Use of the Internet and Dartmouth's computer network and associated resources for one's own commercial gain, or for other commercial purposes not officially sanctioned by Dartmouth College.

When an employee is terminated, that person's account will automatically be deactivated within 4-6 weeks. If a department head or supervisor makes a request, and at the discretion of the Vice President for Information Technology, the account of an already terminated employee may be immediately deactivated. Alternately, a terminated employee could be granted a Sponsored Account if they engage in a continuing relationship with Dartmouth that requires some type of Dartmouth account.

Student accounts are transitioned to alumni account approximately 60 days after they graduate. If a class Dean makes a request, and at the discretion of the Vice President for Information Technology, the account of a student who has officially withdrawn may be immediately deactivated.

In nearly all instances, ITC will not grant requests by department heads, supervisors, or class deans to deactivate the account of an employee or student due to a performance or behavioral issue. Such issues should be resolved by other means, and ITC will not apply sanctions to control behaviors unrelated to computing and the use of information technology. Exceptions will be made as required by law or to avoid a danger to health or safety.

This policy will be enforced and matters falling under it will be adjudicated by the Vice President for Information Technology, who, when appropriate, may consult the Provost.

Appendix

The programs and services on the *Exempted Programs* list below collect information about the people who use them, but are not required to warn of this fact when the program is used. This list is maintained by Information Technology & Consulting and is typically reviewed annually by the Council on Computing at its first fall meeting.

Any program not included on this list that collects information that could directly or indirectly identify a person using the program must warn each user that such information collection is about to occur and must give the user a chance to leave the program before data collection begins. Dartmouth Information Technology & Consulting cannot guarantee that programs not provided by ITC adhere to this provision.

EXEMPTED PROGRAMS

HOST SYSTEMS

All host operating systems on campus (UNIX, Windows, etc.) keep a log of the account numbers of the people or devices that connected to that host, their connect and disconnect times, what programs they run, the amount of computer resources consumed, etc. This information is used for system administration and billing.

EMAIL

Blitz/Office 365 and associated mail systems keep a log of the names of the people who have connected to the mail system, their connect and disconnect times, information about client machine capacities, and summary information about (but not the text of) messages sent or received.

KEYSERVER

The KeyServer keeps a log of the names of people who have connected to the server, their network addresses, their connect and disconnect times, and the names of the KeyServer-controlled software that they used.

NETWORK INTEGRITY

Information Technology & Consulting, with prior contact with specific users as appropriate, may at its discretion run various network programs that help ensure network integrity and security. Such programs may access various files, typically files related to operating systems, on central or distributed computers on Dartmouth College's digital data network.

CANVAS

On occasion, Canvas system administrators need to simulate users' login to Canvas for troubleshooting purposes. By contacting Canvas Support, users agree to allow Canvas system administrators to simulate users' access to Canvas in order to provide adequate support.

Other than when contacted for support by Canvas users, and in accordance with Dartmouth's Information Technology Policy, Canvas system administrators will not simulate any user's login without the user's explicit permission.

Canvas system administrators do not use, or have access to, users' Dartmouth passwords. Furthermore, Canvas system administrators never request a user's password. It is advised that users should be extremely diligent in the protection of their password.

This information and access privileges are not shared with anyone other than the Canvas system administrators group