

# Denison University Acceptable Use Policy

This policy is divided into four sections:

- I. **Guiding Principles** provides background and relates the Policy to the University mission.
- II. **Acceptable Use Policy (AUP)** is the statement of Policy itself.
- III. **Procedures** specify detail for implementing the Policy.
- IV. **Frequently Asked Questions** uses common examples to specifically address issues covered by the AUP.

## I. Guiding Principles

### 1. What Denison Provides and Why

Denison University provides access to a broad range of computing and network services to members of the University community so that they may make productive and innovative use of information technologies. These network services are intended for University-related purposes, including direct and indirect support of the University's instructional, research and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas among members of the Denison community and between the community and the wider local, national and global communities.

Network resources are provided on an "as is" basis. Denison University makes no guarantee that these resources will be free of objectionable material, errors, bugs, viruses, worms or other malicious features. The University is not responsible for any harm arising from the use of network resources, nor is it responsible for any third-party content accessed via the network services it provides.

### 2. Rights, Privileges, and Responsibilities Associated with Campus Network and Computing Resources

The rights of academic freedom and freedom of expression apply to the use of Denison University network resources. This philosophy is based on the belief that information has its greatest value when shared appropriately. Used appropriately, network services maintain and enhance the University's mission; used inappropriately, network services can be used to break laws or infringe on the rights and beliefs of others. Thus, the rights of access to Denison's network resources are balanced by the responsibilities and limitations associated with those rights.

The privilege of access to Denison's network resources is conditioned on acceptance of the responsibilities and limitations associated with that privilege. Users are bound by the

terms of the Acceptable Use Policy whenever they make use of computing or network resources governed by the Policy. This information resource is the shared responsibility of all members of the Denison community. Consistent with other University policies, an individual's right of access to network services should not be denied or abridged because of race, color, religion, ethnic or national origin, age, disability, gender, sexual orientation, or veteran status.

The use of Denison's network resources, like the use of any other University provided resource and like any other University-related activity, is subject to University policies and all requirements of legal and ethical behavior within the Denison community. Thus, conduct that is illegal or inappropriate in the physical world or a violation of University policy is illegal, inappropriate, or a violation when conducted online. Uses of computers or network resources are not acceptable just because they are technically possible.

### **3. Copyright Issues**

The Constitution of the United States (Article I, Section 8) states the purpose of copyright as follows: "To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." In today's interpretation of copyright, Denison recognizes that dual purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorized use or sale of works available in the private sector.

### **4. Applicability**

This policy applies to all users of Denison's computing and network resources, whether affiliated with the University or not, whether the use or access itself is authorized or unauthorized, and to all uses of those resources, whether on campus or from remote locations. In this context, computing and network resources are defined broadly to include, but are not restricted to, access, storage and dissemination of digital media, digital communications and network services of all sorts, including those conducted over wireless networks. Additional policies may apply to specific computers, computer systems, or sub-networks at Denison or to uses within specific departments.

This policy is not a complete statement of Denison University's rights or remedies, and the policy does not waive any rights or remedies of the University. This Policy is subject to change at any time. The current version shall be posted on the Denison University web site. The University may provide users with additional notice of significant changes. Continued use of the network services and resources constitutes acceptance of the revised Policy.

## **II. Acceptable Use Policy**

- 1. All users of Denison University computing and network services must comply with the following statements.**

- **Compliance with Law and University Policies**

Users must comply with all federal, Ohio, and other applicable law; all generally applicable University rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit “hacking”, “cracking”, and similar activities; the University’s policy handbooks; the University’s sexual harassment and non-discrimination policies; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

- **Authorizations**

Users must access only those computing resources they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned. Users who share access to accounts with third parties will be held liable for any consequences caused by third parties’ use of their accounts.

- **Privacy**

Users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access another person’s account does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and obtaining them before proceeding.

- **Consumption of Resources**

Access to University computing and network resources is granted for purposes consistent with Denison’s mission and for limited personal use. Users must respect the finite capacity of computing and network resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Denison may require users of the resources to limit or refrain from uses of specific resources in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

- **Non-commercial uses only**

Users must refrain from using computing and network resources for personal commercial purposes. Personal use of University computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

- **Disclaimer requirement for individual, non-Denison resources and activities**

Users must refrain from stating or implying that they speak on behalf of the University and from using University trademarks and logos without authorization to do so. Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University. Authorization to use University trademarks and logos on University computing resources may be granted only by the Office of Public Affairs, as appropriate. A disclaimer indicating responsibility for content must be presented on all opening screens of network services including web homepages that are operated by individuals or organizations using an IP address assigned to Denison. Failure to include the disclaimer may result in suspension of network connectivity for the service.

## **2. Enforcement and Sanctions**

Users who violate this Policy may be denied access to Denison's computing and network services and may be subject to other penalties and disciplinary action, both within and outside of the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Campus and Residential Life. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

The University may temporarily suspend or block access to an account prior to the initiation or completion of such procedures when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, or availability of University or other computing resources, or to protect the University from liability. Under carefully prescribed circumstances, Denison reserves the right to limit access to network resources and to access data stored on University-owned systems in order to ensure the stability and availability of network resources for the common good of the community.

## **3. Security and Privacy**

Denison University employs various measures to protect the security of its computing and network resources including user accounts. Users must be aware, however, that the University cannot guarantee such security. Users should therefore engage in "safe

computing” practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users must also be aware that their uses of Denison’s network services cannot be considered completely private. The normal operation and maintenance of the University’s computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The University does not routinely monitor an individual’s content or pattern of usage of network resources. The University may specifically monitor the activity and accounts of individual users of University computing and network resources, including individual login sessions, content and communications, without notice, when (a) the user has voluntarily made them accessible to the public, as by posting to a web page, public file sharing application, electronic discussion forums, etc.; (b) it reasonably appears necessary to do so to protect the confidentiality, integrity, or availability of University or other computing resources or to protect the University from liability; (c) there is reasonable cause to believe that the user has violated, or is violating, this Policy or another written University policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law. Any such individual monitoring of content or communications, other than that specified in “(a)”, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance in writing or email by a member of the Denison senior staff or their designee.

The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies under the direction of a court of law and may use those results in appropriate University disciplinary proceedings.

### **III. Procedures**

#### **1. Basic access to computing and network resources**

*(“Computing and network resources” include but are not restricted to, email, storage on campus file servers, the Denison campus network, University-provided computers, web services, networked printers, software, Internet resources, online resources maintained by the Library, etc.)*

Access to secured network resources requires a means to identify and authenticate the user. Usually that is accomplished by assigning a specific account protected by a password. The account owner is responsible for all actions originating from an assigned account. Passwords to protected accounts may not be shared. Use of this assigned account implies that the user understands and agrees to abide by all provisions of the acceptable use policy in effect at that moment. Wherever possible, all Denison login

dialogs will include: “By using this account, I acknowledge that I am aware of and agree to abide by all provisions of the current Acceptable Use Policy.”

Employees of the University who, by the nature of their work, require access to network resources will be assigned a unique username and password. This account will normally be established when the employee begins work, but at the request of the employee’s supervisor, the account may be established as soon as Human Resources verified that the employee is hired. The account will be created automatically and the account owner notified in writing of their username and password. Account usernames will be created based on a syntax that is consistent for the Denison community. Accounts may include but are not limited to administrative system software accounts, email accounts, network accounts, web access accounts and library system software accounts.

All students will be assigned a unique username and password. This account will normally be established as soon as the student accepts admission to the University. The account will be created automatically and the account owner notified in writing of their username and password. Account usernames will be created based on a syntax that is consistent for the Denison community. Accounts may include but are not limited to administrative system software accounts, email accounts, network accounts, web access accounts and library system software accounts.

Campus visitors who are participating in University sanctioned events may obtain a temporary Denison account through the Denison event sponsor. An event sponsor may obtain temporary accounts by contacting the Help Desk or through instructions posted at [www.denison.edu/offices/computing](http://www.denison.edu/offices/computing). All temporary accounts are set to expire immediately upon event termination.

## **2. Access to Library resources**

Library patrons who are not affiliated with the University may be given temporary access to appropriate resources by the Library staff through generic patron accounts. Many online resources of Denison University’s Library are accessible openly through any network connection. Many commercial databases are accessible only to members of the Denison community through on-campus network connections and through remote connections to Denison’s network. Licenses and contracts with commercial suppliers of these databases require that Denison limit access to current students, faculty and staff only. Any effort to breach the protection schemes for limiting access to these resources is a violation of the Acceptable Use Policy.

## **3. Access to additional network resources**

Additional network services may be requested by contacting the Help Desk. Additional services include but may not be limited to the following:

- Space on a Denison web server for departmental, academic, student or University-affiliated organizations, or personal use;
- Shared work spaces;
- Increases in mass storage quota.

#### **4. Deletion, suspension and termination of accounts**

Accounts assigned to employees are subject to deletion immediately upon termination of employment unless prior arrangements have been made and approved by the former employee's supervisor.

Accounts assigned to students are subject to deletion ninety days after graduation or withdrawal from the University unless specific arrangements have been made and approved by the Office of Student Affairs.

Assigned accounts may be suspended (*i.e.*, inaccessible to the user) immediately and temporarily under three circumstances:

- Upon recommendation of the appropriate judicial body in writing or email sent to the Information Security Officer (email: [ITSecurity@denison.edu](mailto:ITSecurity@denison.edu));
- When Information Technology Services staff responsible for systems management have credible evidence that continued use of an account constitutes a threat to the confidentiality, integrity, or availability of computing systems;
- To protect the University from liability.

Every reasonable effort will be made to notify the Director of Information Technology Services as soon as possible of any such suspension.

- When the account is inactive for 180 (one hundred and eighty) days or more;
- Assigned accounts may be terminated immediately and permanently upon the recommendation of the appropriate judicial body in writing or email sent to the Information Security Officer (email: [ITSecurity@denison.edu](mailto:ITSecurity@denison.edu)).

An individual whose assigned account has been permanently terminated may not seek to have a new account assigned to them without approval of the appropriate judicial body.

#### **5. Reporting suspected violations of the Acceptable Use Policy**

Reports about suspected violations of the Acceptable Use Policy should be lodged with the Information Security Officer (email: [ITSecurity@denison.edu](mailto:ITSecurity@denison.edu)). Details of all reports, including the identity of the complainant, will be handled in the strictest of confidence. Anonymous reports may be investigated but are not likely to result in judicial action or resolution.

## 6. Procedures for gathering and reporting evidence

Any office receiving a complaint about a suspected violation of the Acceptable Use Policy will provide an incident report to the Information Security Officer (email: [ITSecurity@denison.edu](mailto:ITSecurity@denison.edu)). Authorizations are required before specific evidence can be gathered about an individual's activity unless required by law or necessary to respond to a perceived emergency situation. Authorization for monitoring an individual's use of resources or the gathering of evidence from an individual's assigned account, network storage space or a University-owned computer must be granted by the appropriate authority. In the case of student accounts, authorizations come from the Vice President for Student Affairs or his/her designee. In the case of members of the faculty, authorizations come from the Provost or his/her designee. In all other cases, authorizations come from the Director of Human Resources.

Alternatively, the Provost may issue authorizations for student or employee accounts. Authorizations must be specific and delivered in writing or by email to the Information Security Officer (email: [ITSecurity@denison.edu](mailto:ITSecurity@denison.edu)) before any evidence is gathered from an individual's accounts. Procedures for gathering of evidence from personally-owned computers in residence halls are defined in the Student Handbook.

Privileges to access computing and network services may be suspended during an investigation of a complaint upon the recommendation of the appropriate judicial body.

Evidence may be reported to the appropriate judicial body or law enforcement agencies for further action. Judicial procedures are defined in the following applicable University handbooks:

- Student Handbook [www.denison.edu/student-affairs/handbook](http://www.denison.edu/student-affairs/handbook)
- Faculty Handbook [www.denison.edu/provost/handbook](http://www.denison.edu/provost/handbook)
- Support Operating Staff Handbook [www.denison.edu/human\\_res/policies](http://www.denison.edu/human_res/policies)
- Administrative Staff Handbook Available from Human Resources

## 7. Registration requirements for personally provided network services

It is technically possible for individuals to operate network services from computers connected to the Denison network. Such services include, but are not limited to, web servers, file transfer protocol (FTP) servers, email servers, wireless access points and more. These services can be operated from both University- and personally-owned computers; they can be private or publicly accessible.

All such personally provided network services must be registered and assigned an appropriate network address. Unregistered network services can disrupt the integrity of the entire network and will be disconnected when discovered. Requests for permission to operate network services must be submitted to the Help Desk.

## **8. Disclaimer requirements for student organization and personally provided network services**

Student organizations that are recognized by the Denison Campus Governance Association (DCGA) and organizations that are affiliated with the University may request resources to operate a web site on the Denison web server. Student organizations requesting such services must first obtain approval by the Campus and Residential Life Office. Authorization for services may then be sent to the Help Desk. Other organizations affiliated with the University must first obtain approval by a sponsoring Denison department. Authorization for services may then be sent to the Help Desk. Content and maintenance of network services sponsored by organizations are the responsibility of the officers of the organization. Content and maintenance of personally provided network services are the responsibility of the individual running the service.

The following disclaimer is required to appear on or be linked from the opening screen of all organization and personally-provided network services, including the home page of personal web sites hosted in the Denison domain: *“Disclaimer: The views and opinions expressed in this service are strictly those of the information provider. The information provider assumes full responsibility and liability for the content of this service. The contents of this service have neither been reviewed nor approved by Denison University. All comments and feedback should be sent to [email address of the provider].”* Services sponsored by organizations or individuals that do not display or link to this disclaimer can be removed from the Denison web server or disconnected from the network.

## **9. Negligent computer use**

It is a violation of the Acceptable Use Policy for anyone to continue to operate any computer on the Denison network that is known to propagate any potentially disruptive software code. Ignorance of technical methods to update, patch or disinfect a computer is not justification for continued use. It is the responsibility of the computer user to take all reasonable steps to ensure that any vulnerable or infected computer on the network is restored to a secure operating condition.

## **IV. Frequently Asked Questions regarding the AUP**

### ***Q. Am I permitted to share my account name and password with another student or another employee?***

A. No. This is strictly forbidden in all circumstances. There are always better ways to handle access to information or resources for another student or employee. Consult with a Help Desk representative to address your information access needs but do not share your account name or password.

### ***Q. Who owns my data?***

A. Data generated in the course of employment belongs to the University. This includes all email. Specifically, identity or proprietary data, whether in paper format, email

oriented, web, or other, is owned by the University, which shall not share it with outside entities.

***Q. May I use my Denison email account to sell a product or service?***

A. No. Denison email services are to be used in support of the University mission and are expressly non-commercial.

***Q. May I copy and/or transport data from the Denison email directory or the Denison web directory to another system for the purpose of sharing the information external to Denison?***

A. No. This is an express violation of the AUP.

***Q. Is my University email private?***

A. Email service is a privilege offered by the University. In practice, Information Technology Services manages University systems and respects each user's privacy. Individual email accounts are considered confidential and will not be monitored or shared unless abuse of the service is suspected, reported, or otherwise authorized to be investigated by a member of Denison senior staff or legal authorities.

***Q. Is my social security number at risk for exposure?***

A. Social Security numbers are collected and stored in University systems as required for federal or state purposes. Social Security numbers are not used for identification purposes. Consequently, every effort is made to reduce the risk of external exposure. It is a violation of the AUP for Denison employees to store social security numbers individually and/or electronically.

***Q. What about my student record? Who uses it and is it safe?***

A. University student records are protected under the guidelines of the Family Educational Rights and Privacy Act (FERPA). Select University employees are authorized to access student records for educational purposes only. Under the AUP, authorized users of electronic student records are strictly forbidden from sharing account names and passwords to University systems.

***Q. Am I permitted to download music or video?***

A. Downloading any material whether text, audio, or video is permitted provided it does not violate the AUP.

- Copyright infringement is a violation of the AUP as it may violate local, state, and/or federal laws.
- Excessive use of Denison bandwidth is prohibited. Depending on the size of the download, the process may be in violation of the AUP.
- As stated in the AUP, use of network services may not be acceptable just because they are technically possible.

***Q. How do I report an AUP violation?***

A. Notify the Information Security Officer (email: [ITSecurity@denison.edu](mailto:ITSecurity@denison.edu)).

**Q. If my Internet service is suspended due to an AUP violation, what do I do?**

A. Follow the instructions provided in your disconnect notice. Contact the Help Desk with any questions or problems in re-establishing the service.

**Q. May I install my own wireless access point on the Denison network?**

A. No. These devices may conflict with the Denison campus-wide wireless network and could also impede network operations for other Denison users.

For questions or feedback, contact: [Lisa Bazley, Director of Information Technology Services](#).

## Revision History

*This policy was developed and is maintained by the Information Technology Advisory Committee.*

*Updates:*

*March 2007 - General revisions*

*June 2010 - Department name changed from "Computing Services" to "Information Technology Services."*

*June 2011 - Wording revisions and addition of the Information Security Officer role.*

*Dec 2011 - Clarify FAQ email statements.*