

**Drake University**  
**Faculty and Staff Policy on Acceptable Use of Computer Technology**

Rev. 10/7/2005

**1. Purpose**

It is the intent of Drake University to provide a quality technological environment for the University community in which certain standards are observed. Use of University technology resources is a privilege and not a right. Therefore, use of such resources is contingent upon compliance with University policies and standards and all governing federal, state and local laws and regulations. All Drake University faculty, staff and guest users authorized to use Drake University computing facilities and services are responsible for reading, understanding and complying with this policy.

**Drake technology resources are available to the following learning communities:**

- i Faculty: see services listed at <http://www.drake.edu/it/> and select *Faculty*
- ii Staff: see services listed at <http://www.drake.edu/it/> and select *Staff*
- iii Alumni: email is available through a service provided by the Alumni Office.
- iv Emeritus faculty: email accounts until there has been one year of inactivity; also access to the Cowles Computer Lab.
- v Organizations with affiliation agreements with the University: as described in the affiliation agreement.
- vi As a depository for federal and state documents, Drake makes library documents available to the Des Moines community at large. Use of public-access computers in the Library for non-research purposes is allowed, if this does not interfere with their primary purpose of providing access for Drake students, faculty, and staff.

**2. Requirements for use of University technology resources**

Users must:

- i Comply with the following Acceptable Use Policy.
- ii Understand and agree that use of Drake University technology resources indicates acceptance of the policy.
- iii Understand that the use of a personally-owned computer that is on the Drake network obligates the owner to comply with the Drake Acceptable Use Policy.
- iv Obtain necessary accounts and passwords and be responsible for maintaining the security of all accounts and passwords.
- v Understand University computer facilities and electronic classrooms are established for educational purposes and those purposes must take priority.

**3. Drake University Acceptable Use Policy**

The purpose of Drake University's Information Technology resources is to support education, research and communication. The following activities are acceptable uses of Drake's information technology environment:

- i Instructional use in Drake University classes
- ii Faculty Research

- iii Student Research
- iv Class Assignments
- v Official work of students, faculty, administration, and staff, recognized student and campus organizations, and agencies of the University
- vi Electronic communication that supports instruction, research, or official work of students, faculty, administration, and staff
- vii Personal use by authorized users that does not interrupt or diminish access to resources for other users and does not violate any applicable law, regulation or University policy.

Additional restrictions apply to use of the Internet over the Iowa Communications Network (see <http://www.drake.edu/it/Policies/ICNProhibitedActivities.html>)

**4. It is a violation of the Drake University Acceptable Use Policy to engage in any of the following behaviors:**

- i Violate the "Statement of Software and Intellectual Rights" (see below). Computer software must be used in accordance with license agreements, whether it is licensed to the University or to the individual.
- ii Violate Copyright Law in any manner, including, but not limited to, downloading copyrighted audio, video, graphics or text materials from the Internet without proof of proper licensing arrangements.
- iii Use another person's account or PIN number or give your password, PIN number or identification to another person for the purpose of gaining access to a University-owned computer, network or database resource. This includes, but is not limited to, unauthorized use of an account, use of an account for a purpose for which it was not intended or use of another person's email address. Changing another person's password may be considered harassment. Users are responsible for safeguarding their identifications and passwords. Each user is responsible for all transactions made under the authorization of his or her ID and password.
- iv Access a file on a University-owned computer or network without the permission of the owner, to copy, rename, modify, or examine it, or to change file protection or visibility. Lack of protection on a file does not imply right of access.
- v Interrupt or inhibit the access of others to Drake University technology resources by actions such as distributing computer viruses, worms, or bulk email. This includes any other procedures that interfere in any way with the information technology resources available to a user. Current virus-scanning software is required for all faculty and staff computers.
- vi Operate a University-owned computer in a manner that is otherwise wasteful of any computing or network resource.
- vii Gain access to Drake University technology resources when one is no longer an eligible user.
- viii Display text or graphic files that reasonably may be considered offensive or which are illegal under obscenity statutes, such as federal law (47 U.S.C. sec. 223(d)) or Iowa law (Iowa Code sec. 728.4). As potential consumers of these materials, users are expected to exercise proper judgment and sensitivity as to how and where these materials are displayed. Users should not be subjected to sexually explicit material, hate literature, or other offensive displays.
- ix Employ a computer to annoy or harass other users; for example, to send obscene, abusive, or threatening mail or email.
- x Use a computer to violate the principles of academic honesty.
- xi Misuse information accessed while performing work as a Drake University employee. Information stored on administrative computers and microcomputers is confidential. Use

- or distribution of such information other than as authorized or assigned is prohibited by University policy and state and federal laws.
- xii Access or attempt to access any of the University's administrative systems and records unless explicit permission has been granted by the Data Owner or their designee; read, delete or in any way modify any such data without explicit permission; distribute, publish or in any way make known any such data to unauthorized persons.
  - xiii Use University-owned computer resources for commercial work except as permitted by faculty and staff handbooks and licensing agreements.
  - xiv Tamper with computers, printers or any other associated University-owned equipment. Remove, without authorization, computer equipment, disks, paper documentation, data or other technology resources.
  - xv Connect any device, other than a computer or printer (e.g., game console, network hub or router, etc.) to Drake's computer network.

## **5. Consequences of failing to follow Drake University Acceptable Use Policy:**

Failure to follow the terms and conditions set forth in this Policy constitutes an offense. As with all matters of law and ethics, ignorance of the laws and rules does not constitute a defense nor excuse violations.

Users learning of suspected policy violations should notify their immediate supervisor, who will notify the CIO and the appropriate department head.

- i. In the case of proven staff and faculty violations, the appropriate department head will consult with the Data Owner concerned regarding the severity and impact of any proven violation. Depending on the severity of the offence, penalties may include expulsion for students and termination for employees.
- ii. A violation of the terms and conditions of this Policy may result in immediate denial of computer/network access or service and/or penalties that range from the loss of computing privileges to termination from the University.
- iii. Policy violators are liable for any monetary payment or damages and may also be subject to civil or criminal prosecution under state and federal laws and regulations.
- iv. The Office of Information Technology will not provide support to users who fail to follow the Acceptable Use Policy.

## **6. Statement of Software and Intellectual Rights**

The following statement, jointly developed by EDUCAUSE, a national consortium of universities concerned with information technology, and ADAPSO, a computer and software services industry association and published in "Using Software: A Guide to Ethical and Legal Use of Software for Members of the Academic Community", is used with permission.

*"Respect for intellectual labor and creativity is vital to academic discourse and enterprise, this principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.*

*Because electronic information is volatile and easily produced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."*

## **7. Privacy and compliance with state and federal law**

Drake University seeks to protect computer-based information, recognized as a primary administrative, educational and research asset, from accidental or intentional unauthorized modification, misuse, destruction, disruption or disclosure. In support of its effort to protect the integrity of its computing systems, workstations, networks, lab facilities, etc., the University has the right to monitor its computing facilities. The University has the right to monitor any and all aspects of its systems, including individual login sessions, to determine if a user is acting in violation of University policies or state and federal law.

## **8. USA PATRIOT Act notice**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA Patriot Act”) expands the authority of local, state and federal law enforcement to gain access to educational records, including stored electronic data and communications. The USA Patriot Acts also expands the ways in which law enforcement officials may track Internet usage and conduct computer network surveillance.

- i When the University receives an order, warrant, subpoena or other request for stored electronic data or communications or to perform surveillance, the University shall request a copy of the document specifying what records are requested or what tracking or surveillance is authorized and will comply with any and all requests in a timely manner. The University may consult with legal counsel prior to the release of any records or prior to authorizing any surveillance.
- ii The University will inform the person whose stored electronic data or communications have been requested or obtained, unless doing so would violate any statute, court order, warrant or subpoena. If the University provides information to the government or allows the government to conduct surveillance pursuant to a USA Patriot Act request, the University may not notify anyone, including the person whose information is being provided or whose information is under surveillance. The University will not disclose to third parties the fact that information has been requested or obtained on an individual or that surveillance has been conducted, unless the individual consents or the University is compelled to make the disclosure by order, warrant, subpoena or other process.

## **9. Disclaimer**

Drake University does not warrant that the functions or services performed by or that the information or software contained on the University’s technology resources will be kept confidential, meet the user’s requirements or that the resources will be uninterrupted or error-free or that defects will be corrected. The University does not make any warranties, whether express or implied including, without limitation, those of merchantability and fitness for a particular purpose, with respect to any technological products or services or any information or software contained therein.