

## Office of Information Technology

# RESPONSIBLE USE OF IT RESOURCES

---

### **POLICY STATEMENT**

---

The use of University information technology resources—like the use of any other University - provided resource and like any other University-related activity—is subject to general expectations of legal and ethical behavior within the University community. This Policy is intended to be an addition to existing University rules and regulations and does not supersede or modify any other University policy, rule, or regulation.

### **REASON FOR POLICY**

---

This document constitutes the University policy for the management of its computer networks, computers, and other devices connected to those networks and the resources made available thereby. Drake University acquires, develops, and maintains information technology resources to support the University's instruction, research, and service missions; University administrative functions; student and campus life activities; and the free exchange of ideas among members of the University community and between the University community and the wider local, national, and world communities.

### **ENTITIES AFFECTED BY THIS POLICY**

---

This policy applies to all users of University information technology resources, regardless of their affiliation with the University, and to all users of those resources, whether on campus or from remote locations. Additional policies may apply to specific information technology resources provided or operated by specific units of the University or to users within specific units. Members of the University community who use resources not owned by the University must adhere to this Responsible Use policy when conducting University business.

### **WHO SHOULD READ THIS POLICY**

---

- All faculty, staff, students, and affiliates of Drake University.

### **WEBSITE ADDRESS FOR THIS POLICY**

---

Drake University Policy Library: [www.drake.edu/governance/policies.php](http://www.drake.edu/governance/policies.php)

Office of Information Technology (OIT) Published Policies: [oit.drake.edu/security-policy](http://oit.drake.edu/security-policy)

**Office of Information Technology**  
**RESPONSIBLE USE OF IT RESOURCES**

---

**TABLE OF CONTENTS**

<b>POLICY STATEMENT</b>	<b>1</b>
<b>REASON FOR POLICY</b>	<b>1</b>
<b>ENTITIES AFFECTED BY THIS POLICY</b>	<b>1</b>
<b>WHO SHOULD READ THIS POLICY</b>	<b>1</b>
<b>WEB SITE ADDRESS FOR THIS POLICY</b>	<b>1</b>
<b>I. RELATED DOCUMENTS, FORMS, AND TOOLS</b>	<b>3</b>
<b>II. DEFINITIONS</b>	<b>3</b>
<b>III. RESPONSIBILITIES</b>	<b>3</b>
<b>IV. PRINCIPLES</b>	<b>3</b>
<b>V. PROCEDURES</b>	<b>3</b>
<b>1. COMPLIANCE</b>	<b>3</b>
<b>2. AUTHORIZATION</b>	<b>4</b>
<b>3. RESOURCE CONSUMPTION</b>	<b>4</b>
<b>4. PERSONAL OR COMMERCIAL USES</b>	<b>4</b>
<b>5. CONTENT</b>	<b>5</b>
<b>6. COPYRIGHT</b>	<b>5</b>
<b>7. PRIVACY</b>	<b>6</b>
<b>8. ENFORCEMENT</b>	<b>7</b>

**Office of Information Technology**  
**RESPONSIBLE USE OF IT RESOURCES**

---

**I. RELATED DOCUMENTS, FORMS, AND TOOLS**

---

University Policies and Documents Applicable to All Units of the University

**II. DEFINITIONS**

---

**III. RESPONSIBILITIES**

---

All members of the Drake University community are responsible for adhering to these standards of use.

All information technology employees are expected to interpret this policy and provide user education where necessary.

**IV. PRINCIPLES**

---

Responsible, acceptable use always is ethical, reflects academic honesty, is consistent with Drake University's mission and values, and demonstrates community awareness regarding the consumption of shared resources.

**V. PROCEDURES**

---

When using Drake University's information technology resources, users are expected to adopt the following practices:

**1. COMPLIANCE**

Comply with all federal, Iowa, and other applicable law; applicable University rules and policies; and all applicable contracts and licenses. Users must comply and not violate laws of defamation, 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; published University policies

**Office of Information Technology**  
**RESPONSIBLE USE OF IT RESOURCES**

---

governing student, faculty, and staff conduct; and all applicable licensees, laws, regulations, and policies.

## **2. AUTHORIZATION**

Use only those information technology resources that are authorized for use on the campus network and use them only in the manner and to the extent authorized by access privileges inherent in the provision of an authorized Drake ID. All users of Drake information technology resources must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Accounts, passwords, and access to University information technology resources may not, under any circumstances, be shared with, transferred to, or used by persons other than those to whom they have been assigned by the University. All Drake University community members are responsible for their uses of University information technology resources on and off campus and for ensuring that their systems are maintained and used so they do not endanger, impede access to, or threaten the privacy or security of others' information or systems.

## **3. RESOURCE CONSUMPTION**

Respect the finite capacity of information technology resources and be mindful of activities that decrease bandwidth and interfere unreasonably with the activity of other users. The University may require users of information technology resources to limit or refrain from specific uses in accordance with this principle. The University will judge the reasonableness of any particular use in the context of all of the relevant circumstances.

## **4. PERSONAL OR COMMERCIAL USES**

Unless designated by college or school policy as an activity relevant to professional development and scholarly work, faculty, staff, and students should refrain from using information technology resources for commercial purposes or for personal financial or other gain. The use of Drake University's information technology resources for personal use is recognized as a common practice within the

## Office of Information Technology

# RESPONSIBLE USE OF IT RESOURCES

---



post-secondary community and is permitted within reasonable limits. Usage must be in accordance with the *University's Political Activity Policy* and cannot be for partisan political activity in the support of or opposition to a candidate for public office at the federal, state or local level even if the candidate is not affiliated with a political party. Such use should not consume a significant amount of those resources, interfere with job performance or other University responsibilities, interfere with the efficient operation of the University or its information technology resources, and must be otherwise in compliance with this Policy. The University assumes no responsibility for the loss or recovery of personal files.

## 5. CONTENT

Drake cherishes the diversity of opinion that is inherent to academic institutions and is respectful of all forms of freedom of expression including academic freedom and freedom of the press. The University does not condone censorship. As a result the University cannot protect individuals against the existence or receipt of material that may be offensive (or immoral) to them. However, users should exercise proper judgment and be sensitive to how materials they display will be perceived by others.

Moreover, we expect compliance with existing law and obscenity statutes. In particular, users should not display material of any sort that is illegal under Federal (e.g. U.S.C sec. 233(d)) or Iowa law (Iowa Code sec. 728.4).

Examples of prohibited content include (but are not limited to) phishing, spamming, or viruses.

## 6. COPYRIGHT

Use must comply with applicable copyright law pertaining to the use, distribution, or reproduction of copyrighted materials, including but not limited to music or video files. Unauthorized use or distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject user to civil or criminal liabilities. United States copyright law provides for a variety of potentially severe sanctions related to copyright infringement, including injunctions, impounding, and disposition of infringing articles,

**Office of Information Technology**  
**RESPONSIBLE USE OF IT RESOURCES**

---

monetary damages (either actual damages or statutory damages of up to \$30,000 for each work infringed), recovery of attorneys' fees and costs, and criminal sanctions under certain circumstances. The University is also required by law to investigate claims of possible copyright infringement taking place through its computer networks. Internal University sanctions for unauthorized use or distribution of copyrighted material range from warnings to the loss of privilege of use of University information technology resources.

## **7. PRIVACY**

Understand that uses of information technology resources are not completely private. Under normal circumstances, University counsel and the individual's dean/director or vice president, in consultation with the Chief Information Officer (CIO), will approve in advance any individual inspection other than that which is voluntary, required by law, or necessary to respond to emergency situations. The University, in its discretion, may use or disclose the results of any such inspection, including the contents and records of individual communications, as it considers appropriate to University personnel, third parties, or law enforcement agencies.

The normal operation and maintenance of the University's technology resources require backup and caching of data and communications, logging of activity, monitoring of general use patterns, and other such activities that are necessary to provide service.

The University does not condone the inspection of personal files or activity. However, the University may determine circumstances that require inspection of files or activity. Examples of such circumstances may include (but are not limited to):

- a) To protect the integrity, security, or functionality of University or other information technology resources, or to protect the University from harm;
- b) There is reason to believe that the user has violated, or is violating, any Drake University policy or applicable civil or criminal law; or

**Office of Information Technology**  
**RESPONSIBLE USE OF IT RESOURCES**

---

- c) An information technology resource appears to be engaged in unusual or unusually excessive activity, as indicated by monitoring of general activity and usage patterns.

## **8. ENFORCEMENT**

Discipline of those who are suspected of policy violations should begin with notification of their immediate supervisor, who will notify the CIO and the appropriate department head. Violations of this policy are considered to be a significant offense. Violators of this policy will be subject to the applicable disciplinary processes and procedures of the University that apply to students, faculty, and staff, and violators may lose their computing privileges and be subject to other measures, up to and including expulsion from the University or loss of employment. Illegal acts involving University information technology resources may also subject violators to prosecution or other sanctions by local, state, or federal authorities.

All decisions regarding the impact on information technology functions and resources shall be made in consultation with the Chief Information Officer.

## **9. 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.

– 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.

**Office of Information Technology**  
**RESPONSIBLE USE OF IT RESOURCES**

---

– 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.