

## **Acceptable Use of Computing and Information Technology Resources Version 2, December 3, 2006**

---

### **Purpose**

The purpose of this policy is to outline the acceptable uses of computing and information technology resources for the Case Western Reserve University community. This policy outlines the standards for acceptable use of University computing and information technology resources that include, but are not limited to, equipment, software, networks, data, and telecommunications equipment whether owned, leased, or otherwise provided by Case. This policy is intended to reflect the University's commitment to the principles, goals, and ideals described in the Case Vision Statement and to its core values.

### **Coordination with other policies and law**

Users of information technology resources at Case Western Reserve University are subject to applicable federal, state, and local laws, applicable contracts and licenses, and other university policies, including those for Human Resources, and those contained in the faculty and student handbooks, and notably those policies governing copyright and intellectual property compliance. Users are responsible for ascertaining, understanding, and compliance with the laws, rules, policies, contracts and licenses applicable to their particular uses. Any case of policy conflicts will be addressed by the policy review process.

### **Access to and Expectations of Persons Using Information Technology Resources**

It is the policy of Case to maintain access for its community to local, national and international sources of electronic information sources in order to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Case maintains a variety of information technologies for use as resources for people, catalysts for learning, and increased access to technology and an enriched quality of learning. Access to this environment and the University's information technology resources is a privilege and must be treated with high ethical and legal standards.

Preserving the access to information resources is a community effort that requires each member to act responsibly and guard against abuses. Therefore, both the Case community as a whole and each individual user have an obligation to abide by the following standards of acceptable and ethical use:

- Use only those computing and information technology resources and data for which you have authorization and only in the manner and to the extent authorized.
- Use computing and information technology resources only for their intended purpose.
- Protect the confidentiality, availability, and integrity of computing and information technology resources, including data.
- Abide by applicable laws and University policies and all applicable contracts and licenses and respect the copyright and intellectual property rights of others, including the legal use of copyrighted material.
- Respect the finite capacity of resources and limit use so as not to consume an unreasonable amount of resources or to interfere unreasonably with the activity of others.
- Respect the privacy and personal rights of others.

## **Acceptable Use Policy**

---

Access to Case information technology and computing resources is a privilege granted to students, faculty and staff of Case. The University extends access privileges to individual users of the University's information technology and computing resources. The extension of these privileges is predicated on the user's acceptance of and adherence to the corresponding user responsibilities detailed in this policy and addendum. The University reserves the rights to limit, restrict, or extend access to information technology resources.

### **Applicability**

This policy applies to all users of Case computing and information technology resources including faculty, staff, students, alumni, guests, external individuals or organizations and individuals accessing external network services, such as the Internet via University facilities. The Vice President for Information Technology Services/CIO will determine operational policies, networking standards and procedures to implement the principles outlined in this policy. ITS has the right to protect shared information technology services.

### **Uses**

In general, the Case community shall use University information technology resources (which include privately-owned computers connected to the University network) in connection with the University's core teaching, research, and service missions. Uses that do not significantly consume resources or interfere with other users also are acceptable, but may be restricted by Information Technology Services. Under no circumstances shall members of the University community or others use University information technology resources in ways that are illegal, that threaten the University's tax-exempt or other status, or that interfere with reasonable use by other members of the University community. Any use of University information technology resources, including network infrastructure, for commercial purposes is prohibited.

### **Sanctions for Violations**

Failure to comply with the appropriate use of computing and information technology resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the secure environment for creating and maintaining information property and subjects one to disciplinary action. Any member of the Case community found using computing and information technology resources in violation of this policy may be denied access to university computing resources and may be subject to disciplinary action, both outside and within the university, including, without limitation, suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate.

### **Privacy and Security**

There is no inherent expectation of privacy for information stored on Case information technology resources, except as provided by federal and state law and other university policy. Every effort will be made to maintain individual privacy, but the university will not be liable for the failure of these privacy efforts. While the university does not routinely monitor individual usage of its computing resources, 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, the scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary for the rendition of service.

### **Review of the Policy**

This policy may be assessed from time to time to reflect substantive change as a result of changes to the Case information technology resources and/or changes in legal statutes that

## Acceptable Use Policy

---

impact information technology resources, copyright, or other intellectual property issues. The Vice President for Information Technology Services is responsible for determining when the policy needs to be reviewed and the process for review and revision.

### Frequently Asked Questions (FAQ)

#### **What is meant by the phrase "...no inherent expectation of privacy"?**

The University provides information technology(IT) and networks with the intent of making information available in an academic setting. Users should understand that this openness brings with it some inherent risks based on the nature of Internet threat sources. Where sensitive information is processed in an official capacity, the IT policies of the university are intended to provide reasonable and appropriate protections to ensure the confidentiality and integrity of such data, while still making that information available to authorized persons.

#### **What if I'm using my personally purchased computer? Does this policy still apply?**

Yes, the policy applies when you are connected to any Case network (wired or CaseGuest wireless) and using the connectivity and bandwidth that Case provides to the community. This policy applies to all information technology resources used to conduct University business, and/or to manage sensitive University information.

#### **What are considered legitimate methods of Case account sharing?**

The practice of individual user account sharing is prohibited.

Case systems have been designed to be self-help by nature. With systems administrators and mailing lists, there are rare instances where a user will legitimately need share their account credentials (CaseID and password). If you share your CaseID and password, you are reminded that your credentials provide access to your payroll, human resources, and benefits functions, as well as email. That means the person you have shared your credentials with can gather your sensitive information and perpetrate Identity Theft crimes against you.

#### **Well, I made a mistake and I did share my account. What do I need to do now?**

To avoid the untoward circumstances of account sharing, you should change your password immediately.

#### **I have observed a violation of this Acceptable Use Policy. What do I do?**

AUP violations should be reported to your manager, department chair, or dean (as applicable) who will then have the option to notify [Case Information Security](#), or calling the Case Help Desk (368-HELP). Depending upon the severity of the violation (e.g. illegal activity, threats of violence, etc.), actions are taken that may include network triage. If an initial investigation produces evidence which indicates an AUP violation has taken place, Case ITS will work through the appropriate supervisory channels. Sanctions for violations are clearly delineated in the AUP document.

If you feel threatened or in personal danger by any online behavior from a Case user via Case IT systems, please call Case Protective Services at 368-3333.

## Acceptable Use Policy

---

### **What is an example of a sanction for a person for violation of the Acceptable Use Policy?**

The University may temporarily suspend or block access to an account prior to the initiation or completion of a disciplinary process when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability.

### **I need to give email sharing permission to my department assistant because I am awaiting a tenure or promotion recommendation and will be out of town. Is this consistent with Case policies?**

The sharing of email and similar information is permitted, it is just the sharing of your user credentials that is prohibited. A viable alternative is to set email forwarding rules to the department assistant, or using a [mailing list](#) or personal alias to share specific incoming mail messages.

### **When the user agreement says that there is routine monitoring, does this mean that my department chair can access my email or hard drive whenever he/she wishes to do so? Don't I have the right to privacy?**

Your department chair cannot access your Case email, network backups, or local hard drive (without your cooperation) under the existing policies without first working through the recognized administrative processes for approval. For faculty, this would mean working through the dean of the pertinent school, then Chief Information Officer (CIO). For staff, Human Resources needs to be involved first and then the CIO is contacted. For graduate and professional school students, either the appropriate dean or Student Affairs would be required to request CIO approval. For undergraduate students, the Dean for Student Affairs would have to approve it before requesting assistance from the CIO.

Any direct active monitoring of individuals by departmental staff without approval is considered to be a violation of the AUP as well.

Routine monitoring means that network usage is noted, unusual connections (indicative of malicious outside users hijacking the current systems) may be investigated, and under those circumstances, email, voice mail, voice connections may be seen by authorized Case employees. The auditing of network and system logs, such as in HIPAA security rule requirements, is another example of routine monitoring. In the event law enforcement needs a right to access, the university cooperates with law enforcement authorities in consultation with the university counsel. There should be no expectation of an inherent right to privacy--such rights cannot be guaranteed within the myriad IT uses at Case. For example, it is possible that emails can be mis-directed or corrupted from a virus.

The only staff authorized to conduct direct active monitoring activities are in ITS, and then only with the focus of investigating a security issue or network use/misuse.

### **What is the process for gaining approval for monitoring of individuals?**

The University may also specifically monitor the activity and accounts of individual users of university computing resources, including individual login sessions and communications, without notice, when (a) the user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly-accessible web page or providing publicly-accessible network services; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of the university or other computing resources or to protect the university from

## Acceptable Use Policy

---

liability; (c) there is reasonable cause to believe that the user has violated, or is violating, this 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, other than that specified in "(a)", required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer's designees.