

# St. Edward's University Technology & Information Policy

## I. Technology Policy

### A. Introduction

1. St. Edward's University provides information technology resources for educational, research, and administrative uses by its students, faculty and staff. This policy supports and supplements the university's more general policies and procedures governing faculty, students, staff, and facilities.
2. University information technology resources that are subject to university policies include, but are not limited to, the following:
  - a. Any computer related equipment and/or data (electronic or printed) owned or managed by the university. This includes electrical power.
  - b. Any computer, server (i.e., any computer that runs an application which allows remote access to local resources), networking device, telephone, copier, printer, fax machine, or other information technology which is owned or leased by the university or is connected to any university network or system is subject to university policies.
  - c. Any device that
    - 1) connects directly to the university data or telephone networks,
    - 2) uses university network-dialup facilities (campus modem pool or wireless systems),
    - 3) connects directly to a computer or other device owned or operated by the university, and/or
    - 4) uses or affects university information technology facilities.
3. Prior to accessing technology in order to post information outside the jurisdiction of the university, you should review the appropriate university policy. Please review
  - a. For staff: the Employee Handbook, "Outside Activities" policy  
<http://www.stedwards.edu/hr/handbook/policies&pro/outact.htm>
  - b. For students: the Student Code of Conduct, Article 2: Misconduct  
[http://www.stedwards.edu/stubook/stu\\_code/poli\\_proc/article2.html](http://www.stedwards.edu/stubook/stu_code/poli_proc/article2.html)
  - c. For faculty: the Faculty Manual, 2.9 Faculty Rights and Responsibilities  
[http://www.stedwards.edu/academic/faculty\\_manual.htm](http://www.stedwards.edu/academic/faculty_manual.htm)
4. Under no circumstances may anyone use information technology resources in ways that are illegal or against university policies, violate the university mission, threaten the university's tax exempt or other status, or interfere with reasonable use by other members of the university community. Violations of information technology rules and policies may result in disciplinary action.

### B. Roles and Responsibilities

#### 1. The University

- a. The university owns most of the computers and all of the internal computer networks used on campus. The university also has various rights to the software and information residing on, developed on, or licensed for these computers and networks. The university administers, protects, and monitors

this aggregation of computers, software, and networks. In its management of information technology, the university and its administrative and academic departments take responsibility for the following:

- 1) Managing computing resources so that members of the university community are not denied fair access to them;
- 2) Establishing and supporting reasonable standards of security for electronic information that community members produce, use, or distribute, and ensuring the privacy and accuracy of administrative information that the university maintains;
- 3) Delineating the limits of privacy that can be expected in the use of networked computer resources and preserving freedom of expression over this medium without permitting abusive or unlawful activities;
- 4) Enforcing policies by restricting access and initiating disciplinary proceedings as appropriate;
- 5) Ensuring that central university computer systems do not lose critical information because of failures or breakdowns;
- 6) Protecting individual passwords from disclosure;
- 7) Providing network access, including wireless access.

## **2. The Individual**

a. All members of the university community must follow the policies that make these resources secure and efficient. All users are subject to university policies and other statements of conduct as published in the Student Handbook, Faculty Handbook, and Employee Handbook as well as all applicable federal, state, and local laws. The University prohibits individual commercial use of university computer systems. Incidental personal use by employees is allowed at the discretion of the cost center manager.

b. Examples of responsible use of technology include but are not limited to the following:

- 1) Observing policies governing the privacy of others, including restrictions placed upon accessible data (secured or otherwise) stored locally or transmitted across network systems;
- 2) Using resources efficiently, and accepting limitations or restrictions on computing resources—such as storage space, time limits, or amount of resources consumed—when asked to do so;
- 3) Backing up files and other data regularly;
- 4) Preventing unauthorized network access to or from their computers or computer accounts;
- 5) Protecting personal passwords and respecting security restrictions on all systems;
- 6) Respecting the rights of others to be free from harassment or intimidation, to the same extent that this right is recognized otherwise on campus;
- 7) Honoring copyright and other intellectual-property rights;
- 8) Taking reasonable precautions to avoid introducing computer contaminants, such as viruses, trojans and worms into university computer systems.
- 9) Honoring academic freedom for professional presentations in public forums and correspondence.

## **II. Information Policy**

### **A. Privacy Policy**

1. St Edward's University complies with all federal and state regulations regarding privacy. SEU will not release non-directory personal data or information to investigators, attorneys, or agencies unless directed to do so by a valid court order. St. Edward's University respects the privacy of users'

electronic files and communications residing on the university's computer system. The university takes precautions to ensure privacy of personal data and information. Personal data will be transferred and stored in a secure manner according to industry practices.

2. Refer to the Roles and Responsibilities section for detail. Individual users of the computer system should be aware of the inherent limitations of shared network resources. No computer security system can absolutely prevent unauthorized persons from accessing stored information, and the university can not and does not guarantee the privacy or confidentiality of stored information or electronic communications.

### **3. Routine Collection of Electronically Recorded Information**

a. Authorized Information Technology personnel may actively scan any computer local to the SEU campus(es) for the purpose of detecting security vulnerabilities on workstations/servers. This is in order to protect Information Technology resources from deliberate or accidental abuse. No other department/user has authorization for this type of activity. The university reserves the right to monitor and access a user's communications, files, and stored information under the following circumstances:

- 1) When necessary to protect the integrity, security, and proper functioning of the university's computing system or to protect the university from liability.
- 2) When required by federal, state, or local law or university policies or regulations as reflected in this policy, Faculty Handbook, Student Handbook, and Employee Handbook.
- 3) When necessary to ensure that high standards of maintenance are met. SEU does not monitor which web sites users visit nor look at what users put in written communications such as emails, news articles, or chat rooms unless an abuse of such services is reported.
- 4) When necessary to tune web server performance and debug problems. Web server logs are primarily used by system administrators and are deleted periodically. However, they may be included on tape backups of the system. These logs typically contain internet address of computer being used, web pages requested, browser used, date and time, and for some applications, user-identifiable information.

### **4. Use/Release of Electronically Recorded Information**

a. St. Edward's University does not attempt to identify individuals or their usage habits. Administration does watch for illegal attempts to upload or alter information, to create conditions that would cause a denial of service or other damage, or to launch attacks on other sites. St. Edward's reserves the right to use web server logs, account records, and other system information to identify the person(s) responsible. Any monitoring or access to a user's files or communications will be no more extensive than is necessary to accomplish the purpose for which it is authorized. Affected users will be notified of such monitoring or access to the extent allowed by law or university policy, provided that it will not compromise the university's investigation or the investigation of any law enforcement organization.

b. Release of electronically recorded information to investigate violations of the Technology and Information Policy and other university policies must be authorized by the appropriate Vice President, with the concurrence of the Vice-President for Information Technology.

## **B. Copyright Policy**

1. The owner of a university computing account or the designated user of a university-owned microcomputer is responsible and liable for respecting all copyright and contractual agreements concerning use and reproduction of software or documentation. Instructional Technology is the university department responsible for maintaining licensing records; consequently, the university

recommends that all software installed on university-owned microcomputers be purchased through Instructional Technology. In the event a user installs, on a university-owned microcomputer, software not purchased through Instructional Technology, that user must forward proof of licensing documentation to Instructional Technology.

2. Use of copyrighted materials, regardless of medium, is subject to all applicable fair use and copyright regulations.

3. Violations of licensing agreements or copyright law will result in removal of copyrighted material and could result in suspension of the user's university computing account.

### **III. Prohibited Uses and Sanctions**

#### **A. Introduction**

1. The university prohibits members of the university community from engaging in any activity that damages data, software or university information technology belonging to the university or to someone else, compromises another individual's ability to use computer-related resources, or disrupts or damages university computer-related resources. When any use of information technology at the university presents an imminent threat to other users or to the university's technology infrastructure, the university may take whatever steps are necessary to isolate the threat.

#### **B. Prohibited Uses**

2. Prohibited uses of university information technology include those

- a. that are illegal;
- b. that are against university policies;
- c. that are disrespectful of St. Edward's mission [<http://www.stedwards.edu/mission.htm>];
- d. that are inconsistent with current Internal Revenue Service (IRS) rulings, that threaten the university's tax exempt or other status, e.g. political use, web advertisement, private commercial use, etc.;
- e. that interfere with reasonable use by other members of the university community, e.g. sending e-mail purporting to come from someone else (e.g., by using someone's logged-in machine);
- f. that interfere with the security, privacy, or responsiveness of networks and systems, e.g. denial of service attacks, hacking, or radio interference from wireless devices, etc.;

#### **C. Sanctions**

1. Use of information technology that violates this policy and rules based on it may result in disciplinary proceedings and, in some cases in legal action. Disciplinary proceedings involving information technology are the same as those for violations of other University Policies, and may be cause for suspension of computing privileges and/or employment disciplinary actions up to and including termination.

2. The university will cooperate with all branches of law enforcement with the identification and prosecution of individuals who act contrary to university policy and the law. SEU cooperates fully with law enforcement agencies, yet there must still be a court order before SEU surrenders user information to external agencies. Information Technology will cooperate with Human Resources and the Dean of Students in the investigation of alleged violations of this policy.

# Appendix

## Key University Policies

Student Code of Conduct: [http://www.stedwards.edu/stubook/stu\\_code/index.html](http://www.stedwards.edu/stubook/stu_code/index.html)

Employee Handbook: <http://www.stedwards.edu/hr/handbook/index.htm>

Faculty Manual: [http://www.stedwards.edu/academic/faculty\\_manual.htm](http://www.stedwards.edu/academic/faculty_manual.htm)

## FERPA

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

## GLB

<http://www.ftc.gov/privacy/glbact/>

## Copyright and Fair Use Resources / Software Licensing

### Primary Sources

U.S. Copyright Office:

<http://lcweb.loc.gov/copyright/onlinesp/>

Digital Millenium Copyright Act:

[http://fairuse.stanford.edu/primary\\_materials/legislation/dmca.html](http://fairuse.stanford.edu/primary_materials/legislation/dmca.html)

Teach Act : [http://fairuse.stanford.edu/primary\\_materials/legislation/teach.html](http://fairuse.stanford.edu/primary_materials/legislation/teach.html)

### Key Copyright Sites:

Copyright Information – St. Edward’s University Library

<http://libr.stedwards.edu/info/copyrightinfo.html>

Copyright Crash Course - University of Texas

<http://www.utsystem.edu/ogc/intellectualproperty/cprtindx.htm>

Copyright & Fair Use – Stanford University Libraries

<http://fairuse.stanford.edu/>

### Additional Copyright Sites:

<http://www.cit.cornell.edu/oit/policy/copyright/>

<http://www.copyright.gov/circs/>

<http://www.educause.edu/issues/issue.asp?Issue=DMCA>