# Acceptable Use Policy

## General Principles

In support of the University of Evansville□s academic mission, the Office of Technology Services supports, facilitates, and empowers access to, and use of, information technology resources. Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Thus, access to the University of Evansville□s computer systems and networks imposes certain responsibilities and obligations and is granted subject to University policies, and local, state, and federal laws.

Acceptable use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals□ rights to freedom from intimidation, harassment, and unwarranted annoyance.

## User Rights

Users granted access to and use of University of Evansville computing resources have certain basic rights. These rights include but are not limited to:

- Freedom of expression.
- Freedom from harassment.
- Equitable share of resources.

It is a violation of the Acceptable Use Guideline for any user to violate these rights.

All users are expected to demonstrate a high level of ethics and regard for others in their access to and use of the campus computing resources. Access to the University□s computing resources is a privilege that may be modified or terminated if a user violates the Acceptable Use Guideline or University policies, or local, state, or federal laws.

## Guidelines

### Acceptable Use

- Use resources only for authorized purposes.
- Access only files and data that are their own, that are publicly available, or to which they have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in their use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

### Unacceptable Use

- The installation or use of unauthorized Wireless Access Points or Routers.

- Displaying sexually-explicit, graphically-disturbing or sexually-harrassing images, text or files in a public computer facility, or location, that can potentially be in view of other individuals.

- Attempting to access another user's computer files without permission.

- Supplying or attempting to supply false or misleading information or identification in order to access another user's account.

- Deliberate, unauthorized attempts to access or use University computers, computer facilities systems, programs, or data.

- The unauthorized capturing of computer network data directly from the network backbone or local area networking media, including wireless transmissions.

- Attempting unauthorized access to computers outside the University using the University's computers or communication facilities.

- Intentionally sending either e-mail or a program that replicates itself (i.e., a virus or worm) or damages another user's account, computer, or operating system.

- Recreational game-playing and/or audio/video file sharing that interferes with instructional or work-related use of university-owned computers.

- Using computer accounts for work not authorized for that account.

- Sending chain letters or unauthorized mass mailings.

- Users will not make, store, transmit or make available unauthorized copies of copyrighted material using the university's computers, networks or storage media. Nor may users use peer-to-peer file transfer services or take other actions likely to promote or lead to copyright infringement.

- Using any Information technology resources, including the University's electronic address (e-mail, web), for personal commercial gain, for charitable solicitations unless these are authorized by the appropriate University officer, for personal political activities such as campaigning for candidates for public office, or for lobbying of public officials. For purposes of this policy, "lobbying" does not include individual faculty or staff sharing information or opinions with public officials on matters of policy within their areas of expertise. Faculty and staff consulting that is in conformity with University guidelines is permissible.

- Using University provided personal web space or email accounts for commercial purposes, other than "classified ad" types of use. (As a rule of thumb, if a classified ad would be appropriate for printing in University Notes, then it is acceptable content for a personal web page.)

- Using the computer for illegal purposes.

- Sending or leaving abusive, obscene messages or content via computer.

- Harassing other users by the sending unwanted messages or files.

- Mass emailing for selling, soliciting, or spamming other users.

- Running unauthorized servers or daemons, i.e., sendmail, named, DHCP, on the network.

- Denying service through any action will not be tolerated.

- Running any unauthorized data packet collection program on the network.

- Attaching any devices to the network without prior approval from OTS is forbidden.

- Unreasonably slowing down the system through the excessive use of bandwidth; deliberately running wasteful jobs, playing games, downloading non-work related video and audio files; running file sharing programs like KaAzA, Gnutella, and others; or engaging in other non-productive or idle network traffic.

- Consuming gratuitously large amounts of system resources (network bandwidth, disk space, CPU time, printer queues, and supplies.)

## *Enforcement*

Minor infractions of this guideline, when likely accidental in nature, such as poorly chosen passwords, overloading systems, excessive disk space consumption, and so on are typically handled in an informal manner by electronic mail or in-person discussions.  More serious infractions are handled via formal procedures.

Infractions such as sharing accounts or passwords, harassment, or repeated minor infractions as described in, but not limited to, the above guidelines may result in the temporary or permanent loss of access privileges.   A student□s academic advisor and/or Student Affairs, or immediate supervisor in the case of a staff or faculty, will be notified in such cases.

More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violation of University policies, or repeated violations as described in the above paragraph may result in the temporary or permanent loss of access privileges.  In all cases, these types of infractions will include notification of a student□s academic advisor and/or Student Affairs, or immediate supervisor in the case of a staff or faculty.

The Office of Technology Services considers any violation of acceptable use guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on University systems allegedly related to unacceptable use. Violators are subject to disciplinary action as prescribed in the student and employee handbooks.  Offenders also may be prosecuted under local, state, and federal laws.

Due to the rapid advances in technology, these guidelines are subject to change frequently.  For the most recent version of this document see http://ots.evansville.edu/.