

# Acceptable Computer Usage Policy

Taylor University owned computer systems exist to assist in the education of Taylor University students. Computer systems are widely used throughout the institution, both in a direct academic environment and in an administrative support role. Administration, education, research and communication are functions that rely on computing and networking technology to accomplish their goals.

It is Taylor University's policy to provide and support computing and network resources to aid in the meeting of goals for institutional programs and purposes, within constraints of budget and time.

The following policy applies to anyone who uses the University's computing and network resources. Note: The paragraphs following each policy statement are intended to be illustrative of the intent of the statement and not intended to be an exhaustive explanation.

## **I. All computer and network usage at Taylor University is a part of community life and therefore the Life Together Covenant applies.**

The Life Together Covenant applies to computing and information resource access especially in the following areas: the access of pornography or gambling on computers, consideration for others and standards of good taste in electronic communications and relationships. This guideline applies to computers found in the various computer lab facilities as well as use of the ResNet residence hall networks.

## **II. All computer and network usage must conform to all University policies and to federal, state and local law.**

Information made available by the university in any electronic format(e.g. Web, e-mail, internal or external) is not to be harvested, distributed or otherwise repurposed without authorization. It is expected that computer users would not, for example, "pirate" software (install a copy of commercial software without paying the license fee), use a pirated copy of a software package or consistently use a "shareware" program without registering it. University plagiarism policies would also, of course, apply to electronic media. This includes unauthorized use, and distribution, of illegal MP3 music or video files.

Information resources must not be used for illegal and/or unethical purposes. Examples include: Intentional harassment of other users; intentional destruction of, or damage to equipment, software, or data belonging to other users; harassment or "stalking" activities; sending e-mail from false usernames; intentional disruption or unauthorized monitoring of electronic communication including the use of password grabbers or network "sniffers". Publishing credit card numbers or passwords to computers or user accounts is also prohibited.

**III. Users must only engage in activities within the intended use of their authorized access and the intended use of any lab or shared system they access. Each lab and shared system will provide specific expectations and priorities of the intended uses for the lab or system, as appropriate.**

Faculty, staff and students are given access to computing, video and voice network resources for specific purposes. Users must avoid activities that are not in accordance with these purposes. Examples of activities which are outside the authorization of all access include: commercial use; attempting to gain unauthorized access to other computers or networks; use of an account on a shared computer or network other than the one assigned to the user. Certain purposes may also have different priorities in the various labs and systems. The same principles apply to the use of the ResNet network from the individual hall rooms.

**IV. Users must be good stewards of the computing and network resources of the University. Each lab and shared system will provide stewardship guidelines for users, as appropriate.**

Many people rely on shared computing resources and a finite bandwidth capacity. Therefore, each user must consider the needs of others when using these resources. Examples of poor stewardship of information resources include: excessive personal use in a lab facility; excessive game playing; where applicable; continuously running "background" programs and reception of large files or running intensive multi-media network applications during "peak" hours. In addition, tying up limited phone resources by staying "dialed out" to local computer services unnecessarily for hours at a time is also inappropriate. These guidelines apply to our life together at Taylor University and are not limited in application to just university-owned equipment. Application can be made to the residential hall network (ResNet) and our Internet bandwidth where applicable.

**V. Users of University messaging systems must be considerate of others. Any attempt to send mass messages that are unsolicited and/or not approved by the University is strictly prohibited.**

It is our desire that the University systems be useful for every user, such as email and portal announcements, be properly managed for every user and that all users are considerate of others. Therefore, the following guidelines are set forth:

-These guidelines address "mass messaging" where the intended recipient does not have a choice in receiving the message and the message is intended for a broad audience, whether internal or external.

-Each Vice President should designate individuals authorized to send mass messages on their behalf. All mass messaging must be sent using only University approved methods.

-All mass messages should include the name and title of the authorized sender. (e.g. Authorized by the Vice President of Academic Affairs)

-Individuals who wish to send a mass message must work through their VP delegated authority.

-All unauthorized mass messages will be considered in violation of the Acceptable Computer Usage policy and the sender may have their access suspended.

**VI. The University reserves the right to limit and regulate any and all usage of its computing equipment and network.**

The University may receive evidence that inappropriate activity is taking place on its campuses. In this event, actions may be taken to investigate the activity. When authorized by the CIO, Director of Technology Services or other appropriate administrators, suspicious computer and network activity may be monitored. As such, electronic mail through the Taylor network and files stored on Taylor's systems should not be considered completely private or confidential. The University also may determine that limiting the individual's access may be necessary. Examples include: removal of a user's account on shared computers; blocking the receipt and sending of electronic mail for a particular user; blocking the user's access to the network(s) even to the point of disabling the physical network connection of their hall room, if participating in the ResNet network. Users of the University's data network must be considerate of others using the same resource. Therefore, any inappropriate or disruptive activity that affects other users whether intentional or not, may also be investigated, and access to the network may be removed as a result. Examples of disruptive use include E-mail spamming, virus attacks, hacking of any kind aimed at any user or system, excessive network traffic bypassing the University's internet filter by using a VPN, and excessive bandwidth utilization.

Violators of these policies may be subject to an institutional discipline process.

Acceptable Computer Usage Policy  
Approved January 10, 2001  
Last Revised August 25, 2006