UNIFICATION THEOLOGICAL SEMINARY
SOCIAL MEDIA AND TECHNOLOGY USE POLICY

Approved: December 14, 2011
Amended: November 28, 2012

Purpose

This document is designed to guide students, faculty and staff in the acceptable use of social media, email, forums, computers, networks, and other information technology resources at Unification Theological Seminary.

1. Social Media: Introduction

Social media (e.g. Facebook, Twitter, blogs), email and other electronic communication tools are quick, easy to use and can have a significant impact on people and the Seminary. Because they are quick and often instantaneous, you need to follow the same ethical standards and laws as you would in face to face communications.

Social Media: Do's and Don'ts

- **Think twice before posting**
  There is no privacy on social media sites. Everything that is being posted can be retrieved by others – even if you delete it immediately. Search engines can find posts years after they were originally posted, people can copy, forward, or otherwise redistribute your posts. If you don't want something to be public – do not post it. If you are emotionally upset, wait until you have calmed down before posting.
- **Be authentic**
  Be honest about who you are. If you are representing UTS in an official capacity, say so. If you post personal views or opinions, state that they do not reflect the views of UTS (e.g. "the post is my own and does not represent UTS position"). Never pretend to be someone else – even "anonymous" posts can be tracked back to the sender.
- **Be accurate**
  Be factual in your postings, especially when representing UTS. Verify your facts, and check for grammar or spelling mistakes. If you make mistakes in content, acknowledge them and post your correction (or retraction). If you change a posting in a blog, say so. You do not want to be charged with changing evidence.
- **Be respectful**
  You want to use the media sites to make your beliefs and opinions known, and this may lead to hot discussions. However, engage in them respectfully, without racial or ethnic slurs, personal insults, or obscenities. You are more likely to achieve your goals if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person.
- **Maintain privacy and confidentiality**
  Do not post private or confidential information about UTS, its students, faculty, staff members or alumni. This pertains to gossip as well as factual information, especially those that may be protected under FERPA (see policy). Please note that you may not post photos/pictures of individuals unless they have given permission to do so.
- **Respect copyright**

When posting follow the same copyright rules as in writing a paper. When in doubt, direct questions to the Library Director (see the UTS Copyright Policy).

- **Protect yourself**
  While you should be honest about yourself, do not provide personal information that can put you at risk.
- **Follow the law**
  You are responsible for your posts, and may be open to charges of libel for content that seems obscene, fraudulent or illegal. UTS reserves the right to delete postings on UTS maintained sites (website, blogs, forum, bulletin boards) that are considered insensitive, harassing or illegal.

Language that is illegal, obscene, defamatory, threatening, infringing of intellectual property rights, invasive of privacy, profane, libelous, threatening, harassing abusive, hateful or embarrassing to any person or entity, or otherwise, is a violation of the student code.

SAFETY & PRIVACY TIPS FOR SOCIAL MEDIA NETWORKING

The internet is open to a world-wide audience. When using social media channels, ask yourself:

1. Did I set my privacy setting to help control who can look at my profile, personal information and photos? You can limit access somewhat but not completely, and you have no control over what someone else may share.

2. How much information do I want strangers to know about me? If I give them my cell phone number, address, email, class schedule, a list of possessions (such as my CD collection) how might they use it? With whom will they share it? Not everyone will respect your personal or physical space.

3. Is the image I'm projecting by my materials and photos the one I want my current and future friends to know me by? What does my profile say to potential faculty members/advisors? Future graduate school/internship interviewers? Potential employers? Neighbors? Family? Parents? Which doors am I opening and which am I closing?

4. What if I change my mind about what I post? For instance, what if I want to remove something I posted as a joke or to make a point? Have I read the social networking site's privacy and caching statements? Removing material from network caches can be difficult. Posted material can remain accessible on the internet until you've completed the prescribed process for removing information from the caching technology of one or multiple (potentially unknown) search engines.

5. Have I asked permission to post someone else's image or information? Am I infringing on their privacy? Could I be hurting someone? Could I be subject to libel suits? Am I violating network use policy or FERPA privacy rules?

6. Does my equipment have spyware and virus protections installed? Some sites collect profile information to SPAM you. Others contain links that can infect your equipment with viruses that potentially can destroy data and infect others with whom you communicate. Remember to back up your work on an external source in case of destructive attacks.

2. Technology Resources: Introduction

Unification Theological Seminary provides students, faculty and staff with technology resources to support the educational mission of the institution. These resources include, but are not limited to computers, computer networks, software and other hardware. Users are expected to use them responsibly and with consideration for the rights and needs of others.

General/Users rights and responsibilities/Use of Hardware or Software

UTS faculty, students and staff may use UTS owned hardware, software, and software licenses under the following conditions:

- Computer use in the Information Commons is restricted to UTS students, faculty and staff. A guest user must obtain permission from the Library Director;
- Users are expected to use electronic resources responsibly. This means among others that users should not be dominate resources and thereby excluding others from being able to use the resources. Users should not share their username and passwords;
- Users have to take responsibility for their own personal data, including backing up files on thumb drives, and properly logging off on public computers;
- Users should be aware of malware (viruses, Trojan horses etc) and take precautionary steps to avoid infection of public computers;
- Only authorized personnel may install programs on Information Commons Computers;
- Users may not change, copy, or delete software unless authorized to do so;
- Users must follow all applicable copyright laws;
- Users who have access to confidential data are being held accountable to protecting this data, especially in regards to the Family Educational Rights and Privacy Act (FERPA) (see UTS FERPA policy);
- Computer hardware may experience mechanical problems at any time resulting in the loss of data;
- Users must use computer and other equipment with care. They are responsible for any damage caused by misuse;
- UTS is not responsible for loss, destruction or damage of personal files;
- UTS periodically deletes all files stored on Information commons computers for security reasons.

Limitations of Use

The use of the resources is a privilege that can be revoked if the user is found to:

- share username and passwords;
- attempt to circumvent security measures;
- intentionally introduce viruses and other malicious programs;
- modify system or network facilities without proper authorization;
- interfere with the ability of others to use the network;
- interfere with the work of another user;
- use Seminary computing resources for malicious or harassing communication;
- obtain unauthorized access to records or data maintained by UTS;

- violate copyright and other federal or state laws;
- do other illegal activities on UTS' resources (e.g. child pornography);
- physically damage technology resources.