



# Acceptable Use of the Internet Policy

September 2017

Date for Policy Review – September 2018

## CONTENTS

1. Acceptable Use of the Internet Policy
2. Internet
3. Email
4. Monitoring

## 1. ACCEPTABLE USE OF THE INTERNET POLICY

This Acceptable Use of the Internet Policy (AUI) applies to all Union School of Theology (UST) staff (including temporary staff), visitors, students and contractors of UST and to all others using the school's IT resources. For the purposes of this document the 'Internet' is defined as; web services, chat rooms, bulletin boards, newsgroups, peer-to-peer file sharing, Virtual Private Networks, Instant Messaging systems, Weblogs ("Blogs") and Social Networking or Social Media sites using company facilities. This policy should be considered part of the Conditions of Use for Computers and Networks at UST.

## 2. INTERNET

### ***2.1 Internet use***

- Use of the Internet by UST staff is permitted and encouraged where such use supports the goals and objectives of the school.
- Internet access is to be used in a manner that is consistent with the school's standards of conduct and as part of the normal execution of an employee's job responsibility.
- Use of the Internet and other facilities is a privilege not a right, and may be withdrawn if deemed appropriate.
- Use of the Internet is monitored for legitimate security and network management reasons. Users may also be subject to limitations on their use of such resources.

- The use of computing resources is subject to UK law and any improper or illegal use will be dealt with appropriately. Legal authorities can have a right of access to electronic data in pursuit of a suspected crime.

### **2.2 Users should never:**

- Visit Internet sites that contain racist, obscene, hateful or other objectionable materials or encourage others to do so on their behalf.
- Make or post indecent remarks, proposals or materials on the Internet including racist, obscene, hateful or sexist jokes and defamatory comments or encourage others to do so on their behalf.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to the school or other third parties, unless this download is covered or permitted under an agreement.
- Intentionally interfere with any implemented anti-virus, anti-spy ware, anti-phishing, anti-pharming, firewall or other security protection measures
- Download any software without the express permission of the Resources Manager, or without using appropriate security measures.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the facilities.
- Use another person's PC to carry out any of the above.

### **2.3 Users should:**

- Make the Resources Manager aware if you find that there has been unauthorised access to your computer.
- Record any instances where you have accessed inappropriate sites by accident. For example this may be through mistyping an address or a "Spam" email link.
- Log out of the computer when you have finished working and lock the terminal if you leave the desk.

UST reserves the right to block or restrict access to certain types of web sites or specific web addresses or domains.

## **3. EMAIL**

### **3.1 Use of email**

- Email is to be used in a manner that is consistent with UST's standards of business conduct.
- Use of email is a privilege not a right, and may be withdrawn if deemed appropriate.

- UST will directly access staff/students email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation. Legal authorities can have a right of access to electronic data in pursuit of a suspected crime.
- Use of email may be subject to monitoring for legitimate security and / or network management reasons. Users may also be subject to limitations on their use of such resources
- The distribution of any information through UST's network is subject to the scrutiny of UST. UST reserves the right to determine the suitability of this information.
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately.

UST reserves the right to redirect the email of staff who leave (for legitimate operational purposes). UST may also block incoming mail from certain addresses or domains.

### **3.2 Users should never:**

- Send or receive any material that is racist, hateful, obscene or defamatory or which is intended to annoy, harass or intimidate another person or encourage others to do so on their behalf.
- Represent personal opinions as those of UST.
- Upload, download or otherwise transmit software or any copyrighted materials belonging to UST or to parties outside of UST.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to financial information, databases and the information contained therein, computer network access codes, patent information and business relationships.
- Reply to "Spam" mail
- Overuse the "URGENT" flag as it will lose its value
- "Spoof" the email address to conceal the sender's identity

### **3.3 Users should:**

- Keep emails brief and use meaningful subject lines
- Re-read messages before sending to check for clarity and to make sure that they contain nothing that will embarrass UST.
- Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email.
- Use file compression techniques for large documents or send them using an alternative method.

- Archive effectively – use folders and delete any messages you no longer need.
- Inform the Resources Manager if you receive large quantities of Unsolicited Commercial Email (“Spam”).
- Avoid using email for sensitive or emotional messages or offensive content.
- Take care in drafting emails, taking into account any form of discrimination, harassment, UST's representation, and defamation.
- Users should be careful when replying to emails previously sent to a group to prevent excessive mail posting (“Spews”).
- Log out of the computer when you have finished working and lock the terminal if you leave the desk.

#### 4. MONITORING

The School accepts that the use of the Internet and email facilities, are an integral to work and studies. However, misuse of such a facility can have a detrimental effect on other users and potentially the school’s public profile. As a result, UST monitors:

- The volume of Internet, network and email traffic.
- The domain names and / or IP addresses of Internet sites visited and domain and / or IP addresses of email received.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

We are obliged to monitor to fulfil our responsibilities with regard to UK law. Action as deemed appropriate by the Resources Manager and the COO may be taken.

#### 5. UST DOWNLOAD/UPLOAD LIMITS.

All users of the UST WIFI network are subject to download limits as follows

Type of user	Download limit (per month)	Consequence
Residential user	50GB	1st month – verbal warning 2nd month – dropped to a 1mbps download speed 3rd month – dropped to 56kbps download speed 4th month – 1 week ban from internet usage
Campus student (not living on site)	10GB	1st month – verbal warning 2nd month – dropped to a 1mbps download speed 3rd month – dropped to 56kbps download speed 4th month – 1 week ban from internet usage

Others	5GB	1st month - verbal warning 2nd month - dropped to a 1mbps download speed 3rd month - dropped to 56kbps download speed 4th month - 1 week ban from internet usage
--------	-----	---