978-646-4357
servicedesk@gordonconwell.edu

OFFICIAL ACCEPTABLE USE POLICY

Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to trustees, employees, students, guests, alumni, faculty, adjunct faculty, student workers, contractors and volunteers for performance of their job functions and students for use while on one of the four campuses or working remotely. This access carries certain responsibilities and obligations as to what constitutes acceptable use of GCTS systems. This policy explains how GCTS information technology resources are to be used and specifies what actions are prohibited. While this Acceptable Use Policy (AUP) is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor or the IT Help Desk. Each user is required to read and certify that he or she understands this policy relating to acceptable use of GCTS computer resources.

Purpose

The purpose of this policy is to detail the acceptable use of GCTS information technology resources for the protection of all parties involved. The Acceptable Use Policy is a top-level policy that describes appropriate and general use for Gordon-Conwell Theological Seminary information technology resources. It is meant to describe the appropriate the general behavior the Seminary expects when using technology and encompasses all Seminary technology resources. The purpose of GCTS IT resources is to support the school's goal of theological education. The following policy applies to all users of GCTS IT resources regardless of their affiliation with the school.

Scope

All Gordon-Conwell Theological Seminary employees, faculty, guests, students, temporary workers, volunteers, and contractors are required to review and accept this policy before access to the network is allowed or other Seminary technology resources is granted. This policy applies to all equipment the Seminary owns or leases (this includes non-seminary owned machines that connect through our network). This policy applies to any and all use of GCTS IT

resources including, but not limited to, computer systems, personal mobile devices, email, network, internet access, online resources and the GCTS Internet connection.

Policy

Machine Use

User Roles	Machine provided[1]	Access to needed systems provided[2]
Staff	Yes	Yes
Faculty	Yes	Yes
Adjunct Faculty	No	Yes
Students	No	Yes
Student Workers	Yes	Yes
Alumni	No	Yes
Contractors	No	Yes
Contracted Vendors	No	Yes
Guests	No	Yes
Classrooms and Lecture Halls	No	Yes

1 Systems must be budgeted when implementing a new position. IT will build in replacements between 4-5 years.

2 Access to systems will only be granted based on acceptable use policy being accepted and followed.

Applicability of Other Policies

The policies contained here are not meant overrule other pertinent GCTS policies or any federal, state or local laws. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed. The user should reference related policies including but not limited to the GCTS Social Media Policy & Guidelines and the GCTS Identity Theft Prevention Program Red Flags Rules Policy.

Compliance

This policy is intended to be compliant with applicable federal, state and local laws and regulations including but not limited to the Family Educational Rights and Privacy Act (FERPA). Additionally, this policy is designed to support compliance.

Personally Identifiable Information

Per the GCTS Identity Theft Prevention Program Red Flag Rules Policy, Personally Identifiable Information (PII) is defined as "Information which alone, or in combination with other information, can be used to identify a specific individual. Identifying information includes names (first name and last name or first initial and last name), social security number, date of birth, driver's license number, identification card number, employer or taxpayer identification number, financial account number, or credit or debit card number (with or without required security code, access code, personal identification number or password that would permit access to a person's financial account), unique electronic identification numbers, address or routing code, or certain electronic account identifiers associated with telephonic communications."

E-mail Use

Personal usage of GCTS email systems is permitted as long as A) such usage does not negatively impact the GCTS computer network, and B) such usage does not negatively impact the user's job performance.

- GCTS email distribution lists are for business and academic use and not for personal use.
- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited and in some cases may also be in violation of the GCTS Community Life Statement (contractors are exempt from compliance with the GCTS Community Life Statement).
- The user is prohibited from forging email header information or attempting to impersonate

another person.

- Email is an insecure method of communication, and thus information that is considered PII may not be sent via email, regardless of the recipient, without proper encryption.
- It is GCTS policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Confidentiality

Access to PII, health, financial, & academic data is limited to those with legitimate business or academic need or having legal right to access. Such private data should not be stored on laptops or other portable devices unless absolutely necessary. Exceptions must be approved by the IT department. The data and the device should be encrypted and password protected.

PII must not be A) shared or disclosed in any manner to non-employees of GCTS unless a non-disclosure agreement is in place, B) posted on the Internet or any publicly accessible systems, or C) transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

Recreational Use

Games and music are allowed on the network so long as they do not interfere with the network's business and academic purposes. Network-intensive entertainment during office hours is discouraged and will be throttled. Users should be aware that certain games, videoconferencing (Skype, Google Hangout) and streaming media (such as Netflix, Hulu) can use excessive bandwidth and potentially degrade network performance for all users.

Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. File access is monitored on a regular basis. If a user finds that he or she does not have the appropriate access for his or her job role, then notify the GCTS IT office by emailing helpdesk@gordonconwell.edu.

Unacceptable Use

The following actions shall constitute unacceptable use of the GCTS network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the GCTS network and/or systems to:

- Pornography and torrents are not permitted on the GCTS network.
- Engage in activity that is illegal under local, state, federal, international, or other applicable laws.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to GCTS.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, hacking, or other IT information gathering techniques when not part of the employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations. Passwords are private and should be protected with the same diligence as social security numbers. All users must use their own logins when accessing seminary resources. Users are responsible for all activities done from their account.
- Setup of personal WIFI in buildings where GCTS provides WIFI access. This includes the Boston, Charlotte and Jacksonville campus buildings as well as the following buildings on the Hamilton Campus: Kerr, Goddard, Academic Center and Retreat House. Personal WIFI systems interfere with GCTS network performance for the entire community.

Malware & Antivirus Protection

GCTS IT owned machines will be provided with malware protection. Others are expected to provide their own malware protection and keep it up to date and functional. This includes

students, volunteers, contractors, and any other user who is using his or her personal machine on the GCTS network. Users are responsible for any damage caused by malware on their computer.

Blogging, Microblogging & Social Media

Any blogging activities that are not otherwise covered by other statements in this policy are subject to the appropriate governing departments such as GCTS Human Resources, appropriate Dean's Office, Student Life and Marketing and Communications. Any blogging, microblogging and social media done on GCTS IT systems is subject to the terms of this policy, whether performed from the GCTS network or from personal systems accessing GCTS IT systems. The user assumes all risks associated with blogging, microblogging and social media.

Instant Messaging

The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

Web Browsing

The Internet is a network of interconnected computers of which the GCTS has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. GCTS is specifically not responsible for any information that the user views, reads, or downloads from the Internet. GCTS recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of GCTS systems to access the Internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on GCTS or on the user's job performance.

Copyright Infringement

GCTS systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without authorization by law or permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs and DVDs; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which the user has not already legally procured. This list is not meant to be

exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above.

Expectation of Privacy

Users should expect no privacy when using the GCTS network. Such use may include but is not limited to: transmission and storage of files, data, and messages. GCTS reserves the right to monitor any and all use of the computer network and all systems. To ensure compliance with company policies this may include the interception and review of all data that traverses the network, inspection of data stored on files and folders on any GCTS systems, hard disks, and removable media.

Bandwidth Usage

Excessive use of GCTS bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low GCTS-wide usage.

Personal Usage

Personal usage of GCTS computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on GCTS or on the user's job performance.

Circumvention of Security

Using GCTS-owned computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

Software Installation

Employees are prohibited from installing software on GCTS systems and computers without IT approval. While we cannot restrict users from installing software on their personal devices, extreme caution should be taken when installing any non-GCTS-supplied program. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. Therefore, employees should use caution when installing new software on their mobile devices and be vigilant of malicious intent.

Audits

GCTS must conduct periodic reviews to ensure policy compliance. A sampling of users may be taken and audited against this policy on a yearly basis.

Enforcement

The GCTS Administrative Offices, Student Life, Human Resources and/or Information Technology Team will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, GCTS may report such activities to the applicable authorities. IT reserves the right to disconnect any device from the network that it considers disruptive.

Version Control and Distribution

Updates to this policy will be noted in this section with a summary statement and date. When this policy is revised, the new version will replace the prior version in the Staff Handbook, Student Handbook, Faculty Handbook, the GCTS website and other systems that display the policy.

I have read and understand the Acceptable Use Policy as provided by Gordon-Conwell Theological Seminary. I understand that the GCTS Administrative Offices, Student Life, Human Resources and/or Information Technology Team will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, GCTS may report such activities to the applicable authorities. IT reserves the right to disconnect any device from the network that it considers disruptive.