Acceptable Use Policy

Overview

Acceptable Use, as it refers to College technology, is a statement of the rules created for the purpose of defining what the proper practices are in relation to the use of technology resources. These resources may include use of the intranet, internet, computer and printing devices, electronic communication such as email, social media, mobile devices, data security and confidentiality. They may also include sanctions and steps that will be taken if a policy is violated.

The Christ College of Nursing and Health Sciences (TCCNHS), as a member of The Christ Hospital Health Network (TCHHN), shares and benefits from the technology resources provided and managed by The Christ Hospital. Therefore, TCCNHS is guided by the information security policies created by The Christ Hospital Information Assurance Manager and approved by The Christ Hospital Chief Information Officer.

The use of technology resources creates and expands opportunities that support the efforts of the TCCNHS community to satisfy its mission and vision and to reach its outcomes. Access to these resources is a privilege, and use of them requires the acknowledgement and acceptance of specific responsibilities to ensure that the integrity and security of the systems not be compromised in any way.

The statements that follow reflect that standards and expectations for acceptable use to be adhered to by members of The Christ College, its' constituents, and any authorized user of these resources whether they be on campus or working remotely.

Network Access

Faculty, staff, and students will be provided with accounts and passwords that give access to the College's network and its devices, programs and files, the TCHHN Intranet, and tools for remote access. It is expected that these users will keep logon information secure and confidential. Passwords should not be shared.

Some resources are provided in shared locations. Users are to be respectful of data privacy and only access files that are pertinent to their role at the College. Availability does not always infer permission.

Logging out of all accounts, specifically in shared locations such as the College's Computer Lab, is required to eliminate the opportunity for misrepresentation of identity or access to resources under another's name.

Connecting personal devices to the TCHHN network is prohibited. Access to the public network, Con_Student, is available, and technical support is provided by the Educational Technology Department if constituents need assistance with this resource.

Computing resources are fixed. There are currently no limitations set for individual use of bandwidth or disk storage space on the network. However, faculty and staff at the College must remain conscientious in how they use these resources. Periodic audits of the College's shared storage drive will be made to maximize space. Any activity that is identified as one contributing to poor network performance will also be addressed.

Internet Access

The Internet is a public domain. Network administrators may deem it necessary to block access to some Internet resources and do so through the use of network policies. Users too must be conscientious in their choice of Internet sites. The Internet, as an information source, should be used in conjunction with coursework, research, teaching, communication, academic and professional development. Users may not use the Internet to engage in any illegal or unlawful activities, nor can it be used as a tool that may cause harm to the College.

Computers, Printers, Copiers, Scanners, Fax Machines

Computer desktops are provided in several locations throughout the College for student use. Faculty and staff are provided with personal laptops. Laptops are made available to adjunct faculty and other constituents while at the College. These devices are to be used for authorized, College-related activities.

College computers are installed with the basic software and applications needed to meet the needs of students and faculty/staff. Configurations should not be modified, nor should programs be copied or removed. Additional software should not be installed without permission. Non-College related materials should not be added, nor should devices be used for outside business or commercial purposes.

College constituents should never permit external vendors or support technicians to access College-issued computers for the purpose of troubleshooting or solving hardware problems.

College provided laptops are owned by the College and as such can be retrieved from the user at any time without prior notice and without permission. Content saved to the laptop becomes the property of the College, and the College maintains the right to access this information as it deems appropriate and necessary.

The Educational Technology Department will provide limited support for student, staff, and faculty personal computers as it relates to use of College online programs such as Blackboard or Pageburst (e-books). This may include, but is not limited to guidance for installation, registration, use, and troubleshooting problems.

College computers and laptops are all configured with access to printers. Printing is a network resource and as such should be used responsibly. Printing should be limited to

College and professionally-related documents. Users need to be mindful that the maintenance and support for printers can be expensive, but that proper use of this equipment can keep costs to a minimum. Most of the College's printers include options for efficient printing and are set to do so. These configurations should not be changed unless necessary.

Students may be provided with recommendations for the efficient printing of PowerPoints and are advised not to print their e-books.

Using printers, copiers, or scanners for the purpose of duplicating copyrighted materials without permission is prohibited. A statement of the College's copyright practice can be found in the Student Policies and Procedures section of the College Catalog.

Occasionally, faculty or staff may have the need to print confidential data. There are printers located in the faculty workroom space on each floor. These spaces are restricted to faculty and staff offering a greater level of security. Documents containing confidential data should be sent to one of these printers using the locked print feature. The locked print feature allows the print job to remain in the queue until the person printing the document enters their user id and password to release it.

Confidentiality may also be relevant when faxing information. Cover sheets noting that the data is confidential should be included. If a faculty or staff member is expecting faxed documents that are confidential in content, they should make arrangements to retrieve the fax at the time it is delivered. The fax machines at the College are in secure areas limited to faculty and staff.

Email and Electronic Communication

Outlook email is the official method for electronic communication at TCCNHS. Outlook webmail is available for remote access. All members of the College are provided with accounts. Access to email is authenticated with the same username and password that is used to logon to the network.

Email should be used primarily as it relates to College business and activities. It also can be used for personal communications provided that doing so does not impact negatively on the network's mail system or an individual's work or student performance. College email addresses should not be used in conjunction with personal services such as eBay, shopping services such as Amazon, or for other personal business needs. TCHHN may block incoming and outgoing email messages associated with these types of service providers.

Faculty/staff and students are expected to communicate via Outlook. Mailboxes should be checked at least daily, and responses should be timely.

College email content should be professional. Faculty and staff are asked to add an email signature to include their title, name, phone, reference to the College and/or

Christ Hospital Health Network, phone contact and URL for the College's website. It is recommended that faculty/staff become familiar with the out-of-office feature and use it if they are going to be unavailable for an extended period of time.

Email messages to large groups within the College can be managed with the use of the CON email distribution lists. While this is a convenience, it is important to note that responses, unless otherwise indicated in the original message, should be to the sender only. Mass email should include a subject, contact information for the sender (signature information is sufficient), and nothing, including links to other sources, that is deceptive or misleading.

Attachments to email are acceptable but cannot exceed 5MB. Users must take care in opening emails with attachments or embedded links, especially if the sender is an unfamiliar name. Email attachments can be sources for a variety of malware that can be hidden in the text of the attachment.

The College email is owned by the TCHHN enterprise and as such can be monitored, blocked, or removed at the discretion of email administrators, particularly if there is concern that an email will compromise the security or integrity of the email system. Permission from the user is not required.

Users may not access non-College email accounts such as Hotmail, Gmail, or Yahoo Mail on their College provided devices. Doing so brings risk to the network. If there is a need to view personal mail, then it should be accessed through the public network, CON_Student, using a personal phone, tablet, or computer.

College email should not be used to promote or solicit for activities or events not associated with or supported by the College. Privacy is to be respected, and the use of email distribution lists should be considered under need-to-know situations. The circulation of textual or graphic content considered to be pornographic or obscene is prohibited.

There are security risks associated with College email being sent and received on personal mobile devices due to the sensitivity or confidentiality associated with the content of some mail messages. Therefore, access to mail from mobile devices is limited to the College's faculty and staff. A security access request form must be submitted and approved by a superior with the authorization of the TCHHN Authorization Manager.

Including confidential information in an email is risky. However, within the workplace it is often appropriate to do so. If documents contain identifying information such as birthdates or social security numbers, it may be necessary to encrypt or password protect them before transmitting.

Mailboxes should be monitored by the user and periodically cleaned out of messages no longer needed. This helps in the maintenance and efficiency of the overall mail system by reducing the need for storage and time to backup mail messages.

The email accounts of students receiving their Associate Degree in Nursing (ADN) are terminated at the beginning of the semester following graduation. ADN students use their College email address in conjunction with registering for their licensing exam and correspondence continues post-graduation. The accounts for students receiving their Bachelors of Science in Nursing (BSN) are terminated within the month following graduation. The accounts of students who withdrawn from the College prior to graduation, as well as faculty/staff who leave the institution, are terminated within three days of withdrawal.

For additional information, refer to the TCHHN Email Policy 4.24.117.

Prohibited or Restricted Forms of Electronic Communication or File Sharing on TCHHN Network

Network resources must be safeguarded. Some technology resources incur greater risk than others, and use is therefore restricted.

- Cloud Based Storage – Dropbox, Google Drive, Microsoft One Drive and similar cloud based services may not be used on the TCHHN Network
- Instant Messaging – Non-College provided instant messaging is not permitted on the TCHHN network.
- Peer-to-Peer File Sharing (P2P) -- digitally sharing files from one computer to another and circumventing security firewalls or protection is not permitted.
- Streaming Media – only approved material specific to College courses or activities is allowed.

Mobile Devices – Physical Security

Mobile devices include laptops, tablets, phones, and flash or USB drives, both College provided and personal.

Mobile devices allow users ease, flexibility, efficiency, and can enhance productivity. What must be considered with the use of mobile devices for business in and out of the workplace is the importance of ensuring that the devices be kept safe from loss or theft, and more importantly, the effectiveness of the safety measures on the device to keep the data secure.

A signed document accepting responsibility for College provided laptops is given to each employee at the time their laptop is deployed. Cables with locking mechanisms and keys are also distributed. A brief in-service is provided to demonstrate how the locks are to be used.

Personal devices should not be left unattended. It is recommended that they be placed in drawers, cabinets or lockers when they are not being used. Flash or USB drives should be kept with the owner at all times or stored in a secure place.

Users must remain aware of the risks associated with connecting mobile devices to unsecured networks such as those that may be found in public wi-fi locations. College provided laptops are configured to include software firewalls and antivirus protection. However, it is important to ensure that the device is connecting to the intended site and not being redirected to a site created for malicious purposes.

If a College provided device is lost or stolen, it must be reported to the College's IT Support Specialist immediately.

Mobile Devices – Data Security

Access to mobile devices should be guarded through the use of a logon name and password. This includes tablets and smartphones. Confidential or sensitive data stored on company or removable storage devices should likewise be encrypted.

For additional information refer to the TCHHN Mobile Device Policy 4.24.121.

Information Security

Information Security refers to the steps taken to ensure that the College's student, employee, and constituent information remains protected from unauthorized access, use, scrutiny, copying, distribution, and deletion. Social security numbers or other types of personal information, student health records, financial aid data, usernames and passwords are examples of confidential information that must be protected.

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that ensures protection to students and their education records. TCCNHS adheres to these guidelines.

The College licenses applications from vendors that facilitate student processes as they move through our system. Documentation from Radius, SonisWeb, Blackboard, PowerFAIDS, and School Messenger indicating that each has their own data security practices in place is provided to the College or available online.

Each of the applications includes a user hierarchy which includes an administrator. The role of administrator is to not only manage the program, but to ensure that those who have access to the programs are aware of and respect the confidential nature of the content. Administrators for each program assign profiles or roles to the members allowing sufficient access to perform their job function. It is expected that users will not share or discuss confidential information with others unless approved by a supervisor to do so.

For additional information refer to the TCHHN Confidential Data Policy 4.24.115.

Summary - User Responsibilities

It is the responsibility of all members of the TCCNHS community to use its technology resources respectfully and with integrity. The points below are to serve as guidelines for ensuring that this occurs.

- Understand that access to TCCNHS technology resources is a privilege and that care must be taken to use these resources efficiently and for the purpose for which they are intended.
- Understand that technology resources are finite and must be shared by all members. Conscientious use of disk or storage space and bandwidth are two features that require attention from everyone.
- Understand the importance of maintaining security as it relates to computer access, user passwords, data privacy, and file sharing. Report breeches that may harm or impact the network and/or its users.
- Understand that College hardware and software cannot be modified in any way that might cause disruption to the College, its constituents, or the TCHHN network.
- Understand that all electronic communication must be professional and cannot be used to solicit, distribute, misguide, prank, defraud, or harass the members of the College community in any way.
- Understand that to connect any non-College device to the network, authorization and approval must be granted.
- Understand that any attempt to knowingly circumvent security measures in order to acquire unauthorized access to secure data such as but not limited to student files, employee records or network resources is prohibited and is subject to either dismissal or termination and possibly legal prosecution
- Understand that practices must be in place and adhered to in order that confidential information remain secure at all times.

Let it be stated that Administration retains the responsibility and right to impose sanctions up to and including dismissal from the College of any constituent who fails to adhere to the aforementioned practices of Acceptable Use of College technology resources. The Christ College of Nursing and Health Sciences supports the full enforcement of federal, state, and local legal sanctions.