Information Technology Policy

CORNISH COLLEGE
OF THE ARTS

Developed, Updated & Approved by the
Information Technology Department and
the President's Cabinet

November 2019

Posted: January 14, 2020
Revised: November 19, 2019

Appendix 6

Passed by the President's Cabinet on 11/19/19

Appendix 6 - Information Technology

Introduction and Overview 1.0

Section 1.1 Mission of Information Technology

The primary mission of the Information Technology Department at Cornish College of the Arts is to provide excellent and effective infrastructure and quality support for computer, audio/visual, voice and application services to the College. The Information Technology Department takes on campus-wide leadership in providing guidance, support, and innovation to bolster the College's mission and enable all the departments to meet their goals.

Section 1.2 Preamble

Cornish College of the Arts provides the security and privacy of the data stored on, redirected through or processed by its technology resources. The College encourages the use of these technology resources, however they remain the property of the College and are offered on a privilege basis only.

Management expects all students, faculty, and staff to comply with this and other applicable Cornish policies, procedures, and local, state, federal, and international laws. Throughout this and all subsequent policy, the term "staff" refers to full- and part-time employees, contractors, consultants, temporaries, student assistants, student work studies, volunteers, emeritus faculty, vendors, and other users including those affiliated with third parties who access Cornish technology resources due to their job responsibilities.

The Information Technology Department at Cornish strives to provide computing facilities and network access to all students, faculty and staff. Cornish expects each member of its community who uses Cornish's information technology resources, on any Cornish campus to do so, responsibly, ethically, and in compliance with all policies, relevant laws, and all contractual obligations to third parties. *If a member of the Cornish community fails to comply with these policies, relevant laws, or contractual obligations, that member's privilege to access and use of Cornish's information technology resources may be revoked.*

Students living in Cornish's Residence Halls should be aware that the Cornish IT Department treats the Residence Halls as an extension of the Cornish campus. This and all subsequent IT Policies are in effect at all times.

Section 1.3 Privacy

Cornish reserves the right to monitor, duplicate, record and/or log all use of Cornish technology resources with or without notice. This includes but is not limited to e-mail, Internet access, keystrokes, file access, logins, and/or changes to access levels. Students, faculty, and staff shall have no expectation of privacy in the use of these technology resources.

Section 1.4 Liability

Cornish makes no warranties of any kind, whether expressed or implied for the services in this policy. In addition, Cornish is not responsible for any damages which students, faculty, and staff may suffer or cause arising from or related to their use of Cornish technology resources. Students, faculty, and staff should recognize that Cornish technology resource usage is a privilege, not a right, and that the policies regarding said usage mandate adherence.

RESPONSIBILITIES AND ACCOUNTABILITY 2.0

Section 2.1 For Students

Students are accountable for their actions and therefore they own any event occurring during the use of Cornish information technology resources. Access of personal or private Internet Service Providers while using Cornish provided information technology resources or using non-Cornish provided information technology resources to conduct Cornish business does not exempt any student from the responsibilities, accountability, and/or compliance with this or other Cornish policies.

Student responsibilities include but are not limited to:

- Access and release only the data for which you have authorized privileges and a need to know (including misdirected email).
- Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer use.
- Report information security violations to the Information Technology Department and cooperate fully with all investigations regarding the abuse or misuse of Cornish owned information technology resources.
- Report (sexual) harassment, intimidation, or other to Title XI or Student Life.
- Protect assigned or personal user passwords, printing codes, and other access keys from disclosure.
- Use only company acquired and licensed software.
- Follow all applicable procedures and policies at all times.

Section 2.2 For Faculty and Staff

Effective information security requires faculty and staff involvement as it relates to their jobs. Faculty and staff are accountable for their own actions and therefore they own any events that occur while using Cornish technology resources. It is faculty and staff's responsibility to abide by all policies and procedures of all networks and systems with which they communicate. Access of personal or private Internet Service Providers while using Cornish provided information technology resources or using non-Cornish provided information technology resources to conduct Cornish business does not excuse any Cornish community member from the responsibilities, accountability and/or compliance with this or other Cornish policies. Faculty and staff responsibilities include but are not limited to:

- Access and release only the data for which you have authorized privileges and a need to know (including misdirected email).

- Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer system use.
- Report information security violations to the Information Technology Department and cooperate fully with all investigations regarding the abuse or misuse of information technology resources.
- Report (sexual) harassment, intimidation, or other to Title XI Officer.
- Protect assigned or personal user IDs, passwords, printing codes, and other access keys from disclosure.
- Abide by all data protection and disclosure laws as outlined by the Family Educational Rights & Privacy Act (FERPA).
- Secure and maintain confidential printed material.
- Log off college and/or personal devices before leaving a workstation unattended.
- Use only Cornish acquired and licensed software.
- Follow all applicable procedures and policies.

2.3 Violations of Policy

The College shall investigate alleged violations of policy. With due regard for the right of privacy of users and the confidentiality of their data, the College reserves the right to suspend or modify computer access privileges, monitor network access, examine files, passwords, and accounting information, printouts, and any other material which may aid in an investigation of possible violations. Whenever possible, the cooperation and agreement of the user will be sought in advance. Individuals found in violation of policy may have their user privileges revoked. Violation of local, state or federal statutes may result in civil or criminal proceedings.[1]

Computing and Network Resources 3.0

3.1 Network Connectivity

Any member of the Cornish community connected on campus to Cornish wireless grants the Information Technology Department the right to monitor, log, and track wireless usage, whether connecting to wireless through a Cornish provided machine or on a personal device. Personal ownership of a device does not excuse the abuse of Cornish network and wireless resources. By connecting to Cornish wireless Cornish community members are subject to all rules and regulations that apply to Cornish owned computing devices.

3.2 Student Resource Computing (SRC) Labs and Workstations

Throughout Cornish's campuses, the Information Technology Department provides open computer workstations with printing access and temporary network storage space. For students, Cornish provides

[1] Cornish College of the Arts Student Handbook

several SRC Labs throughout Cornish campuses. This policy applies to all SRC labs and at any common-use workstation located on Cornish's campuses or Residence Halls.

When using *any* of Cornish owned computers on any of Cornish's campuses:

- Do not tamper with the switch settings, move, reconfigure, or otherwise damage terminals, computers, printers or other equipment.
- Do not collect, read, or destroy output other than your own work without the permission of the owner.
- Do not use the computer account of another person with or without permission unless the account is designated for group work.
- Do not copy any copyrighted software provided by Cornish College of the Arts. Users should be aware that it is a criminal offense to copy any software that is protected by copyright.
- Do not use licensed software in a manner inconsistent with the licensing arrangement as provided by Cornish College of the Arts.
- Do not install personal software on computers. If you need software, requests must be put through I.T. and may involve managerial authorization.

Programs and Software

Students may not copy any copyrighted software provided by Cornish College of the Arts. Students should be aware that it is a criminal offense to copy any software that is protected by copyright. Do not use licensed software in a manner inconsistent with the licensing arrangement as provided by Cornish College of the Arts. Furthermore, no student may install any programs or software onto Cornish workstations without permission. For questions about Copyright and downloading, see relevant sections 4.1, 4.2, 4.3, 4.4.

3.3 Faculty and Staff Computing Resources

All members of the community are responsible for any use of computer access accounts assigned to them and any computers connected to the College network registered to them. Resources are provided to the academic and staff departments, distribution determined by the chair or manager. Cornish expects all faculty and staff to respect the integrity of the physical computing facilities and controls, and respect all pertinent policies, laws, licenses, and contractual agreements.

When using *any* of Cornish owned computers or laptops on any of Cornish's campuses:

- Do not tamper with the switch settings, move, reconfigure, or otherwise damage terminals, computers, printers or other equipment.
- Do not collect, read, or destroy output other than your own work without the permission of the owner.
- Do not use the computer account of another person with or without permission unless the account is designated for group work.

- Do not copy any copyrighted software provided by Cornish College of the Arts. Users should be aware that it is a criminal offense to copy any software that is protected by copyright.
- Do not use licensed software in a manner inconsistent with the licensing arrangement as provided by Cornish College of the Arts.
- Do not install personal software on computers or laptops. If you need software, requests must be put through I.T. and may involve managerial authorization.

3.4 Laptop Responsibilities

This responsibility applies to Cornish College of the Arts faculty and staff who are issued a laptop. Each individual receiving a laptop will need to sign an agreement acknowledging responsibility for the device.

Purpose:
Laptops are a necessary tool for many members of our community. Although laptops are convenient due to their portability, they also expose the college to potential risks. Examples of some of the risks include:

- Damage - Laptops are expensive and can be easily damaged. The most common damage occurs from dropping the laptop and spilling liquids on the device.
- Theft and Loss - Given the portability of laptops, they can be easily stolen and expensive to replace.
- Exposure of College Data - Lost or unsecured laptops may unnecessarily expose sensitive data.

Scope:
All Faculty and Staff that are issued a laptop must sign a laptop agreement. The signed agreement will be kept on file at the Information Technology Department.

Expectations and Precautions

- Always carry the laptop with you or keep it in a hidden, secured location. Never leave your laptop unattended especially in a car or open accessible space as these are the most common places from which they are stolen. It is the borrower's responsibility to take proactive measures to prevent theft and damage.
- Employees should make sure that laptops that are kept unattended be within a secure office, be kept in a locked drawer/cabinet, or secured to an unmovable object using a security cable. Security cables will be provided by I.T. staff and can provide instruction on proper usage of the security cable.
- Employees must sign a laptop loan agreement with the I.T. Department.

Sensitive Data:
In the course of working while not connected to the network, it may be necessary to save documents that contain sensitive information like student addresses, social security numbers, and FERPA information. All such documents should be saved on the shared drive and not on the laptop hard drive. I.T. staff will answer any questions regarding what data is considered sensitive and what is not. All sensitive data should be removed from a laptop as quickly as possible in the event the data is inadvertently stored on the hard drive.

Borrower Responsibility:

The borrower is financially responsible for loss of and damage to the laptop and its components if the laptop is less than three years old from purchase date. If the laptop is older than three years, then the expense of the repair will be paid by the college.

- If a laptop or any of its components are determined to be lost or stolen. The borrower will be responsible for replacement costs if the laptop is less than three years old from purchase date.
- If a laptop or any of its components are damaged while in the care of the borrower. The borrower is financially responsible for the damage if the laptop is less than three years old from purchase date.
- Ensure the laptop is logged out and secured by a login at all times while not in use.

The condition of each laptop will be noted each time a computer is checked in or checked out.

The laptop must be returned by the borrower at the last day of their employment or on the agreed due date to the I.T. Department. Laptops not returned by the due date will be considered lost or stolen and the borrower will be responsible for paying the full replacement cost.

Punitive exceptions may be considered on a case-by-case basis on certain instances. Such matters may be referred to the V.P. of Finance or designee.

3.5 Network File and Cloud Storage

Network File Storage

Information Technology provides access to a shared network drive, a common network folder that can be utilized for storing files that need to be viewed and maintained by multiple users or on multiple machines.

Shared storage permissions are maintained by IT. Requests for access to folders should be made through departmental managers, as permission requests must first be approved by the department before being submitted to IT. Cornish-related use takes priority over personal-related use. Since Cornish's technology resources are limited and inadequate to meet both demands, the Cornish IT department prohibits storing personal information on network resources.

Cloud Storage

Cornish's Google Apps for Education provides online storage for files of all type through Google Drive. Using Drive is extremely helpful in making sure you have access to the files you need from any computer and collaborating with others. This is helpful from a file access perspective; however, precautions need, to be taken from a data security perspective.

You should not use Google Apps or similar cloud-based services for storing, transmission or processing of sensitive information due to the risk of inadvertent disclosure. This disclosure can happen by incidentally granting permission to individuals who should not have to access to privileged information. Each member of the campus community is responsible for the security and protection of computing resources to which he or she has access. To mitigate risk of inadvertent disclosure, the shared drive should be used to store privileged and sensitive information.

The following are examples of information that should not be stored on the Google Drive:

- Copyrighted material that you do not have the right to distribute. For more information on copyright materials and fair use, visit the Cornish Library's guide on copyright and fair use laws. (i.e. - books or audio, uploading media to the Google Drive, and sharing them with students without the copyright holder's permission)
- Social security numbers and birth dates associated with a person's name
- Driver's License numbers or Passport Numbers
- Credit card data
- Cornish domain logins (usernames combined with passwords)
- Information pertaining to campus student misconduct
- Anything personal that does not pertain to official Cornish business

Peer To Peer (P2P) and Copyright 4.0

4.1 College Compliance with the Higher Education Opportunity Act (HEOA) Peer-to-Peer File Sharing Requirements

Cornish College Compliance with the Higher Education Opportunity Act Peer-to-Peer File Sharing

The Higher Education Opportunity Act (Public Law 110-315) (HEOA) of 2008 instituted several provisions towards reducing illegal downloading and uploading of copyrighted works through peer-to-peer sharing (P2P).

The Information Technology (I.T.) department of Cornish College of the Arts has taken several steps to comply in good-faith to these new provisions. The three general requirements outlined through these provisions are as follows:

1. An annual disclosure to students describing copyright law and campus policies related to violating copyright law.
2. A plan to effectively combat the unauthorized distribution of copyrighted materials by users of its network, including the use of one or more technology-based deterrents.
3. A plan to offer alternatives to illegal downloading.

Additionally, this Policy intends to mitigate the College's potential exposure to security risks and liabilities associated with the exploitation of P2P applications to illegally use, distribute and/or store copyrighted materials on the College's Network.

Policy Statement

Cornish College of the Arts is committed to preventing, in so far as practicable, the misuse of the College's Computer Network and other Information Technology Resources, including but not limited to, the unauthorized distribution of copyrighted material by Users of its Computer Network. The College intends to maintain the integrity of its Computer Network, without unduly interfering with educational and research use, by utilizing the methods described in Section 4.2 of this Policy.

Prohibited Activity

It is a violation of this Policy to use the College Network or any Information Technology Resource of the College to distribute, download, upload, stream, scan, store or share any material including software, data, document, sound, music, video, picture, design, graphic, game, or any other electronic file when:

(a) the file is copyrighted but distribution to the User has not been authorized by the copyright owner;

(b) the intended use under the relevant circumstances is specified as illegal by any federal or state law, statute, regulation, proclamation, order, or decree;

(c) the User's intent is deployment or introduction of any virus or malware on any information technology Resource.

4.2 Circumvention Prohibited

Users of the College's Information Technology Resources shall not attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the College for the purpose of implementing this Policy.

Policy with Respect to Unauthorized Peer-to-Peer File Sharing

All members of the Cornish College of the Arts community are required to follow the College Policy on Peer-to-Peer File Sharing. This Policy covers all electronic means to transmit, disseminate or store copyrighted materials including e-mail, web pages, and peer-to-peer file sharing software. The Policy also applies to all computers and applications utilizing the College network. Please be sure that you have rights for any material you are making available or sharing on the College network.

The unauthorized distribution of copyrighted material, including unauthorized peer-to peer file sharing, may subject you to disciplinary action as well as civil and criminal liabilities. A detailed description of the College's policies concerning disciplinary actions for the unauthorized downloading and unauthorized distribution of copyrighted material is set forth in the Student Handbook. Students risk losing their computer access privileges due to multiple violations of the policy. With regard to faculty, a detailed description of the College's policies concerning disciplinary actions for the violating federal law is set forth in the Faculty, and Administrative Manual.

Plans to "Effectively Combat" the Unauthorized Distribution of Copyrighted Material

The Director of Information Technology utilizes technology-based deterrents to combat the unauthorized distribution, downloading, uploading, streaming, scanning, storage or sharing of copyrighted material by Users of the College's Network, and periodically confers with the President's Cabinet to ensure that all such technology-based deterrents employed by the College do not unduly interfere with legitimate educational and research uses of the College's Network.

At least one technology-based deterrent will be in use at all times with respect to the College's Network. As determined appropriate from time to time by the Director of Information Technology, technology-based deterrents may include, but are not limited to, one or more of the following:

1. Bandwidth shaping
2. Traffic monitoring

3. Accepting, aggressively pursuing and responding to DMCA notices
4. Using commercial product(s) to reduce or block illegal file sharing.

For the purpose of implementing this Policy, the Director of Information Technology maintains directive authority over all vendors to the College, including those vendors who supply internet services to student housing, to direct that such vendors use appropriate deterrents to reduce or prevent illegal file sharing and other violations of this Policy. When exercising such directive authority, the Director of Information Technology shall consult with the appropriate contract administration officer of the College and ensure that all corrective actions are taken in accord with relevant contract documents.

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

Legal Alternatives for Downloading or Otherwise Acquiring Copyrighted Material

EDUCAUSE
http://www.educause.edu/legalcontent
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

RIAA
https://www.riaa.com/resources-learning/music-services/
The Recording Industry Association of America (RIAA) is the trade organization that supports and promotes the creative and financial vitality of the major music companies.

MPAA
http://www.mpaa.org/contentprotection/get-movies-tv-shows
The Motion Picture Association of America, Inc. (MPAA), together with the Motion Picture Association (MPA) and MPAA's other subsidiaries and affiliates, serves as the voice and advocate of the American motion picture, home video and television industries in the United States and around the world.

Annual Disclosure

The Office of the Student Life is responsible for disseminating annually a notice to enrolled students regarding the institutional information described in this Section. The methods of dissemination of the Notice may include the College web pages, e-mail, orientation presentations, student publications, publication in the Student Handbook and the Compass portal.

4.3 Copyright and Usage

This policy applies to ALL machines that access the Cornish network, personal laptops as well as Cornish computer workstations, on all Cornish campuses, including Residence Halls.

Information Technology understands the needs of artists to create, discover, and share knowledge and information. While we support these needs, we do not support the misuse of the Cornish computer network, including violations of the Copyright Law of the United States. All individuals seeking to use IT resources should have a basic understanding of the Copyright Law.

> Copyright Law Basics from the US government:
> http://www.copyright.gov/circs/circ01.pdf

We encourage students to become familiar with the Copyright Law, and especially the rules regarding "fair use," which allows for the use of limited portions of a copyrighted work, without the permission of the copyright owner, for purposes such as scholarship, research, and criticism. Fair use does NOT mean that if you think it's fair for you to use a work, it's okay.

> Fair Use Guidelines:
> http://www.copyright.gov/title17/92chap1.html#107

4.4 Violation of Copyright Law

Any Cornish community member found in violation of US Copyright Law can expect:

1. Referral to Dean of Student Affairs for judicial conduct. Staff and faculty will be referred to Human Resources.
2. Technology privileges can be revoked, based on the nature of the offense.

Email Policy 5.0

5.1 Student Email

Cornish considers e-mail as an official channel of communication. All students are assigned a Cornish e-mail account and to ensure that electronic communications are received, e-mail will not be forwarded to a secondary address.

Students are expected to check their e-mail on a frequent and consistent basis in order to stay current with College-related communications. Students have the responsibility to recognize that certain communications may be time-critical. "I didn't check my e-mail", error in forwarding mail, or e-mail returned to the College with "Mailbox Full" or "User Unknown" are not acceptable excuses for missing official College communications via e-mail.

PRIVACY

The Information Technology Department must provide express written permission before sensitive information is forwarded to any party outside of Cornish. Note that the College does not provide facilities for sending or receiving confidential messages, as outlined in the Electronic and Communications Privacy Act of 1989.[2] This means that electronic mail messages are not completely secure and their confidentiality cannot be guaranteed.[3] Examples for why e-mail confidentiality cannot be guaranteed are:

- E-mail may be subject to disclosure under law.
- Back-up copies may be retained for periods of time and in locations unknown to senders and recipients even if the student has deleted it from their account of PC.
- In the course of routine systems maintenance, troubleshooting, and mail delivery problem resolution, Cornish IT staff may inadvertently see the content of email message.
- Password protections are advised but cannot be guaranteed.
- Senders can mask their identity.
- Messages can be easily forwarded without permission to individuals or groups, even though it violates copyright law (see section 4.1).
- Forwarded messages can be altered from the original.
- Encryption and digital signatures are evolving technologies and cannot be constantly maintained.
- Once a message is received on a machine outside of Cornish, all of the above concerns continue to apply.

ACCOUNTABILITY

Students may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Students are to take precautions to prevent the unauthorized use of e-mail account passwords. Passwords are not to be shared with others and their confidentiality is to be strictly maintained. In choosing passwords, students should select codes that are difficult to guess and should change them on a regular basis. Information Technology Department strongly advices to enable Google's 2-Step Verification to add an extra layer of security besides a password. Students must maintain the confidentiality of passwords regardless of the circumstances, never share or reveal them to anyone. Cornish Information Technology staff will never ask you for your password and will never ask for login credentials by email.

[2] Title 18, United States Code, Sections 2510 and following.

[3] Because the electronic mail of students may constitute "educational records," it is subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). The College will access, inspect and disclose such records only under conditions set forth by that statute.

Students should contact the Information Technology Department with questions regarding the appropriateness of information sent through e-mail.

Ethical and Acceptable E-mail Use:

- Communications and information exchanges directly relating to Cornish education and opportunities.
- Announcements of Cornish sanctioned events and activities, such as Student Interest Groups, theater, and dance performances, the BFA show and similar approved activities.
- Respecting the legal protection provided by all applicable copyrights and licenses.

Unethical and Unacceptable Use:

- Opening up access to their own account so that people not affiliated with the College can use its resource. Example: Allowing a family member who is not affiliated with the College to use your email service or to access online information services through your account even if these services are publicly available.
- Attempting to obtain unauthorized access to other users' accounts, data, or files.
- Attempting to crack, capture, or use other users' passwords.
- Creating or maintain a file of passwords for any system or network on Cornish computers.
- Sending e-mail messages of a harassing, intimidating, offensive or discriminatory nature.
- Sending in messages that are likely to result in the loss of a recipient's work or data.
- Sending 'chain letters' or 'broadcast messages' to lists or individuals.
- Forging or misrepresenting one's identity in electronic communication for any purpose.
- Misrepresenting your current role and accomplishments at the college.
- Giving the impression you are representing Cornish College of the Arts unless you are authorized to do so.

Google Suite for Education and Cornish

Cornish student e-mail service is provided through Gmail. Students are asked in the first e-mail log in to accept the Terms and Conditions of Google Gmail, and must operate within the rules and regulations mandated by Google as well as those regulated by Cornish. For more information about Gmail's Terms, Conditions and Privacy Policy, go to:

https://www.google.com/gmail/about/policy/

Violation of Cornish's E-mail Policy will result in disciplinary action as outlined in the Student Code of Conduct, and sections 2.1 and 2.3.

5.2 Faculty and Staff Email

Cornish College of the Arts Information Technology Department provides electronic mail services (e-mail) to all current Cornish faculty, staff, and Emeritus E-mail is considered an official channel of communication at Cornish and all faculty and staff are responsible for checking their e-mail on a regular basis.

This policy provides faculty and staff with guidelines for permitted use of Cornish e-mail technology resource. The policy covers e-mail coming from or going to all Cornish owned personal computers, servers, laptops, paging systems, cellular phones, and any other resource capable of sending or receiving e-mail on any Cornish campus, as well as any personal devices that have been configured to access Cornish e-mail.

OWNERSHIP

Cornish owns all e-mail systems, messages generated on or processed by e-mail systems (including backup copies), and the information they contain. Although faculty and staff members receive an individual login to access the e-mail system – all email remains the property of Cornish College of the Arts.

Cornish e-mail must be used to conduct Cornish business and use of Cornish e-mail is only intended for professional Cornish related work. Cornish is not liable for loss of (access to) personal emails on a Cornish account during employment or after departure.

MONITORING

Cornish monitors, with or without notice, the content of e-mail for problem resolution, providing security, or investigating activities. Consistent with generally accepted business practices, Cornish collects statistical data about its technology resources. Cornish Information Technology Department staff monitors the use of e-mail to ensure the ongoing availability and reliability of the systems.

ACCOUNTABILITY

Staff and Faculty may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Staff and Faculty must maintain the confidentiality of passwords regardless of the circumstances, never share or reveal them to anyone. The Information Technology Department must provide express written permission before sensitive information is forwarded to any party outside of Cornish. Faculty and staff should contact the Information Technology Department with questions regarding the appropriateness of information sent through e-mail.

Ethical and Acceptable E-mail Use

- Communications and information exchanges directly relating to the mission, charter, and work tasks of Cornish.

- Announcements of laws, procedures, hearings, policies, services, or activities.
- Notifying students, faculty, and staff of Cornish sanctioned event, such as Staff day, theater performances, staff/faculty luncheons, the BFA show, and similar approved activities.
- Respecting the legal protection provided by all applicable copyrights and licenses.

Unethical and Unacceptable Use

- Violating any laws, Cornish policies or regulations (e.g. those prohibiting sexual harassment, unsanctioned activities, or discrimination).
- Submit, publish, display, or transmit any information or data that contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material.
- Compromising the privacy of staff, faculty, students, or data protected by the Family Educational Rights and Privacy Act (FERPA) and/or using personal information maintained by Cornish for private interest or advantage.
- Spamming (e.g. sending sports pool or other gambling messages, or chain letters).
- Intentionally propagating, developing, or executing malicious software in any form (e.g. viruses, worms, Trojans, etc).
- Viewing, intercepting, disclosing, or assisting in viewing, intercepting, or disclosing email not addressed to you.
- Distributing unsolicited advertising, not pertinent to Cornish business.
- Misrepresenting your current role and accomplishments at the college.

<u>Domain Accounts</u> 6.0

Information Technology provides access to the Cornish domain for current faculty, staff, as well as student work-studies through specialized accounts. These accounts, whether they belong to one individual or are shared by several Cornish community members, grant the user certain privileges: the ability to log onto their workstation, e-mail accounts, the Compass online information portal, and the wireless network. Domain accounts are also linked to copiers for print tracking and accounting, and also grant access to file storage network resources across networks.

Although Information Technology staff will never ask for user credentials over e-mail, it is the responsibility of the user to keep their password safe and not give it to unauthorized people. In the case of shared accounts on common workstations, it remains the responsibility of the user not to compromise the security of the account. Refer to section 2.2.

Password Policy for Domain Accounts

Domain account passwords expire every twelve months. For security reasons, those current Cornish employees with domain accounts are required to change their password at the end of each twelve-month period.

New domain account passwords:

- Cannot be any of the previous three passwords used for the domain account
- Must be 8 characters long
- Must contain 1 number and 1 uppercase letter

Password Policy 7.0

Passwords are a vital part of computer security. Passwords are the first line of defense protecting Cornish data. Therefore, a poorly (weak) chosen password can open up Cornish to risks of unauthorized access to various Electronic Resources like email accounts, online library resources, student information systems, financial records, file repositories, learning management systems, and administrative /transactional systems. The same counts for not keeping the password confident and sharing it with others.

Creating a strong password is important in helping Cornish protecting its data. You can do so by:

- Creating at least twelve characters, (longer is better)
- Inserting a mix of upper and lower case letters (a-z, A-Z), numbers (0-9), and symbols (~!%^)+]>}`$*)
- Something hard to guess, but easy to remember (catchphrase or several random words)

Another action that can be taken is to enable two-step authentication on online (Cloud) accounts. By doing so a second layer of protection is added making it harder to compromise an account. Even when a password is compromised, the second step will block access by requiring a code by text or phone usually.