Cornish Information Technology Policy

INTRODUCTION

MISSION OF INFORMATION TECHNOLOGY

The Information Technology Department at Cornish College of the Arts is dedicated to delivering infrastructure and support services for computing, audio/visual, voice, and applications. We lead campus-wide initiatives to provide guidance, support, and innovation, empowering all departments to achieve their goals and advance the College's mission.

SCOPE & PURPOSE

Cornish College of the Arts is committed to ensuring the security and privacy of data stored on, redirected through, or processed by its technological resources. While the College encourages the use of these resources, they remain the property of the College and are provided on a privileged basis.

All students, faculty, and staff are expected to comply with all Cornish policies, procedures, and local, state, federal, and international laws. The term 'staff' includes full- and part-time employees, contractors, consultants, temporaries, student assistants, student work studies, volunteers, emeritus faculty, vendors, and other users affiliated with third parties accessing Cornish technology resources due to their job responsibilities.

The Information Technology Department at Cornish strives to provide computer and network accessibility to all members of the Cornish community. Users are expected to use Cornish's information technology resources responsibly, ethically, and in compliance with all policies, laws, and contractual obligations to third parties. Failure to comply may result in the revocation of access privileges and/or disciplinary actions.

PRIVACY

Cornish reserves the right to monitor, duplicate, record, and/or log all use of Cornish technology resources without consent. This includes but is not limited to email, Internet access, keystrokes, file access, logins, and/or changes to access levels. This monitoring is conducted to ensure compliance with policies, protect against security threats, and maintain the integrity of the IT infrastructure. Students, faculty, and staff should assume that most activities conducted using these technology resources are public. If individuals have concerns about monitoring or wish to request access to their own monitoring data, they may contact the IT department for assistance.

LIABILITY

Cornish is not responsible for any damages, whether direct, indirect, incidental, or consequential, that students, faculty, and staff may suffer, or cause arising from or related to their use of Cornish technology resources. It is important for students, faculty, and staff to recognize that the use of Cornish technology resources is a privilege, not a right, and that adherence to the policies outlined in this document is mandatory.

RESPONSIBILITIES AND ACCOUNTABILITY

FOR STUDENTS

Students are accountable for their actions and therefore are responsible for any events occurring during the use of Cornish information technology resources. Accessing 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:

- Accessing and releasing only the data for which they have authorized privileges and a need to know (including misdirected email).
- Abiding by and being aware of all policies and laws (local, state, federal, and international) applicable to computer use.
- Reporting information security violations to the Information Technology Department and cooperating fully with all investigations regarding the abuse or misuse of Cornish-owned information technology resources.
- Reporting harassment, intimidation, or other issues to Title IX or Student Life.
- Protecting assigned or personal user passwords, printing codes, and other access keys from disclosure.
- Using only company-acquired and licensed software.

FOR FACULTY & STAFF

Effective information security requires the involvement of faculty and staff in their respective roles. Faculty and staff are accountable for their actions and are responsible for any events that occur while using Cornish technology resources. It is the responsibility of faculty and staff to adhere to all policies and procedures of all networks and systems. Accessing 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:

- Accessing and releasing only the data for which they have authorized privileges and a need to know (including misdirected email).
- Abiding by and being aware of all policies and laws (local, state, federal, and international) applicable to computer system use.
- Reporting information security violations to the Information Technology Department and cooperating fully with investigations regarding the abuse or misuse of information technology resources.

FOR FACULTY & STAFF CONT.

- Reporting harassment, intimidation, or other issues to the Title IX Officer.
- Protecting assigned or personal user IDs, passwords, printing codes, and other access keys from disclosure.
- Abiding by all data protection and disclosure laws as outlined by the Family Educational Rights & Privacy Act (FERPA).
- Securing and maintaining confidential printed material.
- Logging off college and/or personal devices before leaving a workstation unattended.
- Using only Cornish-acquired and licensed software.

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, cooperation and agreement from the user will be sought in advance. Individuals found in violation of policy may have their user privileges revoked and/or be subject to disciplinary actions. Violation of local, state, or federal statutes may result in civil or criminal proceedings.

PASSWORD POLICY

Passwords are a vital part of computer security and the first line of defense protecting Cornish data. Therefore, a poorly (weak) chosen password can open Cornish to risks of unauthorized access to various 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 protect 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 special characters (~!%^)+]>}`$*)
- Something hard to guess, but easy to remember (catchphrase or several random words)

MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor Authentication (MFA) is a requirement across the school to enhance security by adding an extra layer of protection to user accounts. This measure is crucial in safeguarding sensitive information and other Cornish assets, preventing unauthorized access, and mitigating risks associated with cyber threats, such as phishing attacks and data breaches. By requiring users to verify their identity through multiple methods, such as a password combined with a mobile app confirmation or a security token, MFA ensures that even if one credential is compromised, unauthorized access to the system is significantly more difficult, thereby protecting the school's digital infrastructure and personal data of students and staff.

DOMAIN ACCOUNTS

Cornish College of the Arts provides access to the college's domain for current faculty, staff, and student work-study employees through specialized user accounts. These domain accounts grant users the ability to log into their workstations, access email, the Compass online portal, the wireless network, and other resources.

ACCOUNT SECURITY RESPONSIBILITIES

- Domain account passwords expire every 12 months, at which point users are required to change their password for security reasons.
- Users must keep their domain account passwords confidential and secure. Information Technology staff will never ask for user credentials over email.
- For shared domain accounts on common workstations, users are responsible for ensuring the security of the account is not compromised.

SHARED DOMAIN ACCOUNTS

In specific cases, domain accounts may be shared by multiple Cornish community members, such as for student work-study positions. Users of shared accounts are jointly responsible for:

- Maintaining the security and proper use of the account.
- Ensuring confidential or sensitive information is not accessed or stored on the shared account.
- Promptly reporting any suspected unauthorized access or security issues to the IT department.

Failure to adhere to the domain account security requirements may result in disciplinary action, including the suspension or revocation of IT access privileges.

COMPUTING AND NETWORK RESOURCES

NETWORK CONNECTIVITY

Any member of the Cornish community connected, wired and/or wirelessly, on campus grants the Information Technology Department the right to monitor, log, and track all network usage, whether connecting through a Cornish provided assets or on a personal device. The use of personal devices (BYOD - bring your own device) does not excuse or permit the abuse of Cornish College's network and wireless resources. By connecting to Cornish network Cornish community members are subject to all rules and regulations that apply to Cornish owned computing devices.

STUDENT RESOURCE COMPUTING (SRC) LABS

Throughout Cornish’s campuses, the Information Technology Department provides open computer workstations with printing access and temporary network storage space. For students, Cornish provides several SRC Labs throughout Cornish campuses. This policy applies to all SRC labs and to 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 provided by Cornish College of the Arts.
- Do not install personal software on computers. If you need software, requests must be put through Information Technology and may involve managerial authorization.
- Engaging in cryptocurrency activities while using Cornish resources is strictly prohibited.

PROGRAMS AND SOFTWARE

Students, faculty, and staff may not copy any copyrighted software provided by Cornish College of the Arts. It is a criminal offense to copy any software protected by copyright. Do not use licensed software in a manner inconsistent with the licensing arrangement provided by Cornish College of the Arts. Furthermore, users may not install any programs or software onto Cornish workstations without permission.

FACULTY AND STAFF COMPUTING RESOURCES

Users 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 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 remove technology assets from designated rooms and classes without permission from the Information Technology department.
- 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 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 Information Technology and may involve managerial authorization.
- Engaging in cryptocurrency activities while using Cornish resources is prohibited.

LAPTOP RESPONSIBILITIES

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

SCOPE & PURPOSE

All faculty and staff issued a laptop must sign a laptop agreement, which will be kept on file at the Information Technology Department. Laptops are essential tools for many members of our community. While laptops offer convenience due to their portability, they also expose the college to potential risks, including:

- **Damage:** Laptops are expensive and can be easily damaged, with common issues including drops and spills.
- **Theft and Loss:** Due to their portability, laptops are susceptible to theft and can be costly to replace.
- **Exposure of College Data:** Lost or unsecured laptops may expose sensitive data.

EXPECTATIONS AND PRECAUTIONS

LAPTOP LOAN AGREEMENT

- Employees must sign a laptop loan agreement with the Information Technology department before being issued a company laptop.
- 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 the 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 the purchase date.
- The condition of laptops will be formally documented during the check-in and check-out process.
- Laptops must be returned by the borrower on the last day of their employment or on the agreed due date to the Information Technology 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 for certain instances. Such matters may be referred to the Vice President of Finance or their designee.

LAPTOP SECURITY

- Always carry the laptop with you or keep it in a hidden, secured location. Never leave your laptop unattended, especially in a car or other open, accessible space, as these are common targets for theft.

- It is the borrower's responsibility to take proactive measures to prevent theft and damage to the laptop.
- Laptops left unattended must be kept in a secure office, locked drawer or cabinet, or secured to an immovable object using a security cable provided by the Information Technology department.
- Ensure the laptop is logged out or locked while not in use.
- The Information Technology department can provide instructions on the proper usage of security measures.

LAPTOP DATA MANAGEMENT

- When working offline, avoid storing documents containing sensitive information such as student addresses, social security numbers, or FERPA-protected data on the local laptop hard drive.
- Instead, save any necessary sensitive documents on the organization's secure shared network drive.
- Employees should contact the Information Technology department if they have any questions about what data is considered sensitive and requires special handling.
- In the event sensitive data is inadvertently saved to the laptop's hard drive, it should be removed as quickly as possible to minimize the risk of unauthorized access or data breaches.
- Laptops should be configured to prevent users from downloading unauthorized software or changing security settings without Information Technology approval, especially if they may contain sensitive information.
- Employees should be trained in proper laptop security practices, such as never leaving laptops unattended in public and immediately reporting lost or stolen devices.

NETWORK FILE AND CLOUD STORAGE

NETWORK FILE STORAGE

Cornish College of the Arts provides employees with access to a shared network drive. This common network folder are designed for storing and accessing files that need to be viewed and maintained by multiple users or across multiple machines.

The shared network drive is intended for Cornish-related business use only. Storing personal files or information on the shared network drive is prohibited, as Cornish's technology resources are limited and must be prioritized for the college's operational needs.

Permissions to access specific folders on the shared network drive are maintained by the Information Technology department. Requests for access to shared folders must be submitted through departmental managers, as permission requests require approval from the relevant department before being processed by Information Technology.

Cornish-related use of the shared network drive takes priority over personal use. Since the college's technology resources are inadequate to fully meet both business and personal storage demands, the Cornish Information Technology department reserves the right to restrict or remove any personal files stored on the shared network drive in order to ensure it is used effectively for the college's operational needs.

Employees should contact the Information Technology department if they have any questions or need assistance with accessing or using the shared network drive.

CLOUD STORAGE

Cornish's Google Apps for Education, including Google Drive, should not be used for storing, transmitting, or processing sensitive information due to the risk of inadvertent disclosure. The key is to avoid storing any sensitive, confidential, or regulated data on cloud-based services like Google Drive, and instead use the college's secure, on-premises shared network drive for this purpose.

CLOUD STORAGE CONT.

Proper data security and access controls are crucial to prevent inadvertent disclosure of sensitive information.

Examples of sensitive information that should not be stored on Google Drive include:

- Social security numbers, birth dates, driver's license numbers, or other personal identifiers.
- Credit card data or other financial information.
- Cornish domain login credentials (usernames and passwords).
- Information related to student misconduct cases.
- Copyrighted material that does not have permission for distribution.
- Any other personal information not directly related to official Cornish business.

Each member of the campus community is responsible for ensuring the security and protection of computing resources they have access to, including avoiding the storage of sensitive data on cloud-based services like Google Drive.

Employees should contact the IT department if they have any questions about what information is considered sensitive and requires special handling.

PEER TO PEER (P2P) AND COPYRIGHT

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 digital resources, without unduly interfering with educational and research use.

All members of the Cornish College of the Arts community must adhere to the College Policy on Peer-to-Peer File Sharing, which applies to all electronic means of transmitting, disseminating, or storing copyrighted materials, including email, web pages, and peer-to-peer file sharing software. This policy also covers all computers and applications using the College network. It is important to ensure that you have the rights to any material you share on the College network.

Unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may result in disciplinary action and civil and criminal liabilities. Details regarding disciplinary actions for unauthorized downloading and distribution of copyrighted material can be found in the Student Handbook. Students risk losing their computer access privileges for multiple policy violations. Faculty can refer to the Faculty and Administrative Manual for information on disciplinary actions for violating federal law.

HIGHER EDUCATION OPPORTUNITY ACT (HEOA) P2P FILE SHARING REQUIREMENTS

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).

HIGHER EDUCATION OPPORTUNITY ACT (HEOA) P2P FILE SHARING REQUIREMENTS CONT.

The Cornish Information Technology department has taken several steps to comply in good faith with these new provisions. The three general requirements outlined through these provisions are as follows:

- An annual disclosure to students describing copyright law and campus policies related to violating copyright law.
- 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.
- 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.

PROHIBITED ACTIVITY

Employees and students must only use Cornish's IT systems and network for lawful, authorized purposes related to the college's educational and operational needs. Unauthorized or illegal use of IT resources, including the distribution of copyrighted content without permission, is strictly prohibited.

It is a violation of Cornish’s Information Technology Policy to use the college's network or any other IT resource to:

- Distribute, download, upload, stream, scan, store, or share any copyrighted material, including software, data, documents, audio, video, images, or other electronic files, without authorization from the copyright owner.
- Engage in any activity that is specified as illegal under federal or state laws, statutes, regulations, proclamations, orders, or decrees.
- Deploy or introduce any virus, malware, or other malicious code onto Cornish's information technology resources.

PROHIBITED ACTIVITY CONT.

Users of digital resources shall not attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the College. Violations of this policy may result in disciplinary action, including the suspension or revocation of IT access privileges, as well as potential civil and criminal penalties under applicable copyright and cybercrime laws.

STRATEGIES FOR COMBATTING UNAUTHORIZED DISTRIBUTION OF COPYRIGHTED MATERIAL

The Director of Information Technology employs 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. The Director periodically consults with the President's Cabinet to ensure these deterrents do not unduly interfere with legitimate educational and research uses of the College's Network.

STRATEGIES FOR COMBATTING UNAUTHORIZED DISTRIBUTION OF COPYRIGHTED MATERIAL CONT.

Various technology-based deterrents are utilized based on determined misuse. These may include, but are not limited to:

- Bandwidth shaping
- Traffic monitoring
- Accepting, aggressively pursuing, and responding to DMCA notices
- Using commercial products to reduce or block illegal file sharing.

The Director of Information Technology has authority over all vendors to the College, including those providing internet services to student housing. This authority allows the Director to direct vendors to use appropriate deterrents to reduce or prevent illegal file sharing and other violations of this policy. When exercising this authority, the Director consults with the appropriate contract administration officer of the College to ensure all corrective actions align with relevant contract documents.

SUMMARY OF CIVIL AND CRIMINAL PENALTIES FOR VIOLATION OF FEDERAL COPYRIGHT LAWS

Copyright infringement occurs when someone exercises, 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 copyrighted work. In the context of file-sharing, downloading or uploading substantial parts of a copyrighted work without authority constitutes infringement.

Penalties for copyright infringement include civil and criminal penalties. In civil cases, the infringer may be ordered to pay either actual damages or statutory damages set between $750 and $30,000 per work infringed. For willful infringement, a court may award up to $150,000 per work infringed, along with costs and attorneys' fees. Criminal penalties for willful infringement can include imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please refer to the U.S. Copyright Office's website at www.copyright.gov, particularly their FAQ section 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.

COPYRIGHT & 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.

The Cornish Information Technology department 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 Cornish 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 Guidelines:
http://www.copyright.gov/title17/92chap1.html#107

VIOLATION OF COPYRIGHT LAW

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

- Students will be referred to the Dean of Student Affairs for judicial conduct.
- Staff and faculty will be referred to Human Resources.
- Technology privileges may be revoked based on the nature of the offense.

EMAIL POLICY

GOOGLE SUITE FOR EDUCATION

Cornish student email service is provided through Gmail. Students are asked in the first email 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/

OWNERSHIP

Cornish owns all email systems, messages generated on or processed by email systems (including backup copies), and the information they contain. Although faculty and staff members receive an individual login to access the email system – all email remains the property of Cornish College of the Arts. Use of Cornish email is only intended for Cornish related work. Cornish is not liable for loss of (access to) personal emails on a Cornish account.

STUDENT EMAIL

Cornish considers email as an official channel of communication. Students are assigned a Cornish email account, and to ensure that electronic communications are received, email will not be forwarded to a secondary address. Students are expected to check their email frequently to stay current with college-related communications.

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 Communications Privacy Act of 1989. Email messages are not completely secure, and their confidentiality cannot be guaranteed. Examples of why email confidentiality cannot be guaranteed include disclosure under law, retention of backup copies, inadvertent viewing by IT staff, and the evolving nature of encryption technologies. Students should select secure passwords and never share them.

ACCOUNTABILITY

In addition to a password, the Cornish Information Technology Department requires MFA to add an extra layer of security. 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.

Students should contact the Information Technology Department with questions regarding the appropriateness of information sent by email.

ETHICAL & ACCEPTABLE USES:

- 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 & UNACCEPTABLE USES:

- Allowing unauthorized use of your account.
- Attempting unauthorized access to other users' accounts, data, or files.
- Sending harassing, offensive, or discriminatory messages.
- Sending messages results in loss of recipient's work or data.
- Sending chain letters or broadcast messages.
- Misrepresenting your identity or current role at the college.
- Giving the impression you are representing Cornish College of the Arts without authorization.

FACULTY AND STAFF EMAIL

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

This policy provides faculty and staff with guidelines for permitted use of Cornish email technology resources. The policy covers email 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 email on any Cornish campus, as well as any personal devices that have been configured to access Cornish email.

MONITORING

Cornish reserves the right to monitor the content of email, with or without notice, for purposes such as problem resolution, ensuring security, or investigating activities. In line with standard business practices, Cornish also collects statistical data about its technology resources. The Cornish Information Technology Department oversees email usage to guarantee the ongoing availability and reliability of the systems.

ACCOUNTABILITY

Staff and Faculty are accountable for adhering to this email policy. Failure to comply may result in loss of email privileges and/or disciplinary action. It is imperative that staff and faculty maintain the confidentiality of their passwords and never share or reveal them to anyone. Additionally, the Information Technology Department must grant express written permission before forwarding sensitive information to any party outside of Cornish. Faculty and staff are encouraged to contact the Information Technology Department with any questions regarding the appropriateness of information sent through email.

ETHICAL & ACCEPTABLE USES:

- Communications and information exchanges directly relating to the mission, charter, and work tasks of Cornish.
- Announcing laws, procedures, hearings, policies, services, or activities.
- Notifying students, faculty, and staff of Cornish sanctioned events, 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 & UNACCEPTABLE USES:

- Violating any laws, Cornish policies, or regulations (e.g., those prohibiting sexual harassment, unsanctioned activities, or discrimination).
- Submitting, publishing, displaying, or transmitting 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.