Table of Contents

1.1 OUR MISSION

The primary mission of the Information Technology Department at Cornish College of the Arts is to provide effective and quality support and infrastructure for computer, audio/visual, multimedia, voice and application services to the College. The Information Technology Department strives to provide guidance in incorporating new technologies to enable departments to meet their goals.

1.2 PREAMBLE

Cornish College of the Arts provides for 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, retired annuitants, 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 provides computing facilities and network access to all students, faculty and staff. Cornish expects each member of its community to use Cornish's information technology resources, on any Cornish campus, responsibly, ethically, and in compliance with all Policy, 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.

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.***

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.*

2.0 RESPONSIBILITIES AND ACCOUNTABILITY

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 polices 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
- 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 polices

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 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 state owned information technology resources
- 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 information, magnetic media or electronic storage mechanism in approved storage containers when not in use and dispose of these items in accordance with Cornish policy
- Log off systems before leaving a workstation unattended
- Use only Cornish acquired and licensed software
- Attend periodic information security training provided by Cornish
- 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, tapes, and any other material which may aid in an investigation of possible violation. 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 statures may result in civil or criminal proceedings.[1]

---

[1] Cornish College of the Arts Student Handbook 2010-2011

3.0 COMPUTING AND NETWORK RESOURCES

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 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.

SRC Lab Locations

- MCC, 1st floor, computer lab
- MCC, 2nd floor, Library lab
- MCC, 2nd floor, Writing Center
- Kerry Hall, Basement, Student Lounge
- Kerry Hall, 1st floor, 5 common-use workstations

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.

On each SRC lab machine, students have access to and the use of the following programs and software:

- Firefox
- Internet Explorer
- Microsoft Office: Word, Excel, PowerPoint
- Open Office
- PDF Creator
- Adobe Reader
- Paint.NET
- ARTstor: OIV
- QuickTime
- Real Player
- Windows Movie Maker
- CDBurner XP
- VideoLAN: VLC Player

Requests for other software pertaining to Cornish business, school or class work should be made through the I.T. department.

Locations of Department-Specific Labs

The following Department-Specific labs have their own policies, permissions, and programs. As a student of any of the following departments, you may have access to one or more of the labs listed below. For information regarding the policies of Department-Specific labs, please consult with the Department associated with the lab in question.

- MCC, 2nd floor, 212 (Art/Design)
- MCC, 2nd floor, 210 (Art/Design)
- MCC, 4th floor, computer lab (Performance Production)
- MCC, 4th floor, Design Senior Studios (Design)
- MCC, 5th floor, computer lab (Design)

- Kerry Hall, Basement, Digital Music Lab (Music)

3.3 FACULTY AND STAFF COMPUTING RESOURCES

All members of the College 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 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.

3.4 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. Students can access network storage space via any SRC lab computer.

For Students

Because this information is accessed by a large number of individuals, we highly recommend you create your own backups of all documents saved to the shared drive either on personal thumb drives, external hard drives, or by e-mailing documents to your home computer. ***Student shared drive space is intended as temporary storage space only, and should not be used as a permanent place to store files. All files older than FOUR WEEKS from the current date will be deleted.***

Student Guidelines for Network Storage

- In the shared drive, create your own folder and name it with your first and last name.
- Save your documents to this folder, **NOT to the desktop. Files saved to the desktop will be deleted every time the computer reboots, which is at the end of every work day in all open labs**.
- Do not open, move, edit or delete any documents or folders that do not belong to you. Please respect that many other students use the shared drive, and your access to the files does not give you permission to tamper with the work of others.
- All documents are publicly viewable and modifiable. For this reason, do not store sensitive information in networks storage space.
- Some department specific labs may allocate alternative network storage space for their students on those workstations. Consult your department coordinator for more information.

For Faculty

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.

4.0 PEER TO PEER (P2P) AND COPYRIGHT

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

The HEOA includes provisions that are designed to reduce the illegal uploading and downloading of copyrighted works through peer-to-peer (P2P) file sharing. These provisions include requirements that:

1. *Institutions make an annual disclosure that informs students that the illegal distribution of copyrighted materials may subject students to criminal and civil penalties and that describes the steps Cornish will take to detect and punish illegal distribution of copyright materials.*
2. *Certify that we have developed plans to effectively combat the unauthorized distribution of copyright material.*
3. *"To the extent practicable," offer alternatives to illegal file sharing.*
4. *Identify procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials.*

The Information Technology Department at Cornish College of the Arts takes the following steps in order to comply with the HEOA regulations. Below you will find the main HEOA requirements accompanied by a brief outline of what steps Cornish is taking to comply with these requirements.

1. *Make an annual disclosure that informs students that the illegal distribution of copyrighted materials may subject students to criminal and civil penalties and that describes the steps Cornish will take to detect and punish illegal distribution of copyright materials.*

   CORNISH POLICY: *Cornish provides all students with the Student Handbook which is updated annually. Cornish includes this Policy in the Student Handbook as well as posting said Policy on the Cornish website.*

2. *Certify that we have developed plans to effectively combat the unauthorized distribution of copyright material.*

   CORNISH POLICY: *The Information Technology Department at Cornish uses network equipment to identify and block all traffic to peer-to-peer sharing sites on all Cornish networks. In addition, the Cornish IT Department logs connection attempts on all machines that access the Cornish network (personal laptops as well as all computer workstations) and keeps IP records for clients.* If your computer begins to consume excessive network resources, Information Technology will investigate your network activities in order to keep the network operating smoothly.

3. *"To the extent practicable," offer alternatives to illegal file sharing.*

   CORNISH POLICY: *Cornish refers students to* the following extensive list of ***Legal Sources of Online Content,*** compiled by Educause: http://www.educause.edu/legalcontent

4. *Identify procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials.*

   CORNISH POLICY: *Cornish periodically tests current and upcoming peer-to-peer software against our firewall, in order to ensure that our system effectively combats the use of peer-to-peer software for illegal purposes.*

A more detailed HEOA Policy statement and compliance can be found at:
http://www.cornish.edu/campus/information_technology/

4.2 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/circ1.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

4.3 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.

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. Students must maintain the confidentiality of passwords and, regardless of the circumstances, *never share or reveal them to anyone*. Cornish Information Technology staff will not ask you for your password.

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

Ethical and Acceptable E-mail Use:

---

[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.

- 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.
- Practicing good housekeeping by deleting obsolete messages.

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 publically 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.
- Giving the impression you are representing Cornish College of the Arts unless you are authorized to do so.

Google Apps 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:

http://mail.google.com/mail/help/terms.html

http://www.google.com/intl/en/privacy/privacy-policy.html

http://www.google.com/about/corporate/company/privacy_principles.html

http://www.google.com/apps/intl/en/terms/education_terms.html

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 and staff. 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, e-mail and e-mail resources remain the property of Cornish College of the Arts.

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 may be subject to loss of e-mail privileges and/or disciplinary action if found using e-mail contrary to this policy. Staff must maintain the confidentiality of passwords and, 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
- Practicing good housekeeping by deleting obsolete messages

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

---

6.0 DOMAIN ACCOUNTS

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 six months. For security reasons, those current Cornish employees with domain accounts are required to change their password and the end of each six 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