III. ACCEPTABLE USAGE OF COMPUTER SYSTEMS AND FACILITIES

ELECTRONIC COMMUNICATIONS & DATA

This policy applies to Peirce College's Electronic Communications Resources owned, leased, or managed by the College, including, but not limited to, the following:

- All components of the electronic communications physical infrastructure (for example, desktop computers, laptops, servers, routers, and wireless devices).
- All electronic communications and data (for example, staff and student information), or other identifiers associated with the College's systems and services (for example, email addresses and logins).
- Internet access, telephone (office and cellular), electronic mail, fax, photocopying, audio, and video recording, instant messaging and social media (for example, personal websites, blogs, Facebook, Twitter, and LinkedIn; collectively, “Electronic Communications Resources”).

All students are required to use their Peirce College electronic identification (i.e., login) when utilizing a College computer. All users of the College’s Electronic Communications Resources and Technology shall have no expectation of privacy over such use.

Electronic Communications Resources are provided to students for the sole purpose of research and other activities related to College courses.

As an exception to the foregoing limitation, students may use the Electronic Communications Resources for personal purposes, provided that such use:

- is kept to a minimum.
- does not directly or indirectly interfere with the College's operation of the Electronic Communications Resources.
- does not negatively impact a student's work study employment, performance, or obligations to the College.

Students shall not, under any circumstances, use Peirce College Electronic Communications Resources for:

- unlawful activities.
- commercial purposes.
- personal financial gain.
- disruptive purposes or to defame the College or any third party.
- distribution of jokes, personal graphics, video clips, or solicitations.

Students must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Peirce College, unless authorized to do so and limited to student work study-related matters. All authorized electronic communications sent on behalf of the College must contain the College's approved legal disclaimer.

Students must not directly, by implication, or through use of software, employ a false identity (i.e., spoof), or the name or electronic identification of another.

Students must not use Peirce College electronic communications resources for purposes that could reasonably be expected to directly or indirectly cause excessive strain on the College's Electronic Communications Resources or interference with others' use of the College's Electronic Communications Resources. This includes, but is not limited to:

- Sending or forwarding electronic mail chain letters.
- Exploiting electronic communications systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications.
- Sending an extremely large message or sending multiple electronic communications to one or more recipients to interfere with the recipients' use of electronic communications systems and services.
III. ACCEPTABLE USAGE OF COMPUTER SYSTEMS AND FACILITIES

The electronic communication method known as **Instant Messaging** (IM or ICQ) and any derivations of unsanctioned electronic communications tools are not permitted to be used on or in connection with Peirce College’s Electronic Communications Resources, unless configured and installed by a member of the College’s Information Technology Department for College-related educational/research/business and other specifically authorized purposes.

Reasonable efforts are made by the College to filter out unsolicited electronic messages, sent or posted as part of a larger collection of messages, all having substantially identical content, and commonly referred to as “spam.” However, given the nature of the Internet, the College cannot prevent users from receiving electronic communications they might find offensive. The College is not responsible for any harm, loss, or damage incurred by an individual as a result of personal use of or inability to use the College’s Electronic Communications Resources.

The use of cell phones at Peirce College by students, although not prohibited, should not interfere with the learning environment. Cell phone use is not permitted in classrooms under any circumstances. Students taking a call on their cell phone during class must leave the classroom. Cell phones used within the premises of the College must be programmed so that notification of incoming calls cannot be heard by others around him/her.

The use of personal or College owned **Visual Recording Devices** and/or **Audio Recording Devices** are generally not permitted on College premises. Students are further prohibited from recording conversations or lectures at the College or for arranging for or assisting others (students, employees, or non-employees) to do so.

Visual recording devices include, but are not limited to, cameras, video cameras, cellular camera phones, and/or any other device which is capable of taking, storing, or displaying a visual picture, whether in real time or time delayed. Audio recording devices include, but are not limited to, tape recorders, video cameras with audio components, and/or any other device which is capable of capturing, storing, or playing sounds.

Peirce College **Electronic Communications Data**, (which includes, but is not limited to electronic mail, web, PC or server based data, created or owned by the College) must reside on College servers and not on desktops or laptops. In addition, College Electronic Communications Data cannot be backed up nor duplicated onto personal devices. Personal storage devices are strictly prohibited from use on or with Peirce College Electronic Communications Resources. Personal devices include, but are not limited to, Zip drives, USB storage devices, CD/DVD burners, or any other type of personal mass storage device.

Students must comply with the College’s limitations on data storage of electronic communications. Failure to comply with such limitations will result in automatic warning and the eventual inability to use electronic communications until the student reduces data storage to acceptable thresholds.

**Technology Usage**

The term “Peirce College Technology” includes all College-leased, licensed, or owned hardware and software, all College websites, network systems, databases, any online or distance learning system used by the College, and all documentation relating to the foregoing. Activities covered by this policy include, but are not limited to, usage of College applications and the Internet; files, data, and printing; network and/or distance learning system usage; security and confidentiality of data; and passwords.

All Peirce College students must use Peirce College Technology only for course-related educational/research, and other specifically supported purposes. Minimal personal use of Peirce College Technology by students is permitted, provided that such use:
III. ACCEPTABLE USAGE OF COMPUTER SYSTEMS AND FACILITIES

• is kept to a minimum.
• does not directly or indirectly interfere with the College’s operation of Peirce College Technology.
• does not negatively impact other students, faculty, and Peirce College Technology (labs, library, classrooms, wireless, etc.).
• is not for political, romantic, for-profit, or other commercial purposes.

Peirce College students are not permitted to use any Peirce College employee’s telephone or fax without direct and supervised approval of a manager or his/her designee. Long distance telephone and fax calls are paid for by the student when the bill is received by the College.

Under no circumstances may a Peirce College student login at or use a Peirce College employee’s computer.

All students must protect their User Login from unauthorized use. Students are responsible for all activities on their User Login or that originate from their User Login.

A student may access only files, communications, and data that are created by the student, or that are publicly available, or to which the student has been given authorized access. A student is prohibited from accessing, viewing, printing, imputing, deleting or changing any records including his or her own records or those regarding any other student(s) or concerning any Peirce College employee record without proper authorization from the College.

A student may not use or access another student’s or employee’s User Login, password, or email. A student cannot login at more than one computer at a time or allow his or her Login to be used on multiple computers.

All students must abide by all applicable laws and rules, including, but not limited to, copyright laws, software license terms, property rights, website, and Internet service provider terms of use, and privacy laws and policies.

Students must not install, download, or store any software or other electronic content on, or remove any software or data from, Peirce College’s Technology or Electronic Communications Resources. Examples of software or other electronic content include, but are not limited to, music, games, screen savers, commercial shareware, and freeware software.

Students are prohibited from any activity that might be harmful to or compromise the security of Peirce College Technology or any information on Peirce College Technology or Electronic Communications Resources, such as, creating or propagating viruses, Trojan horses, worms, or other invasive or destructive content or software; disrupting services; allowing unauthorized persons to access or use Peirce College Technology; or damaging files; and/or vandalizing any Peirce College Technology or making any attempt to harm or destroy data of another student, faculty, administrative, or staff member.

Students cannot register, sell, or lease College-owned equipment or software for personal profit or benefit. Students shall not connect any non-College owned hardware or software to Peirce College Technology. This includes, but is not limited to, hubs, wireless routers, network cards, external peripheral or external storage, or recording devices (USB, CD, or DVD burners), home computers, PDA’s, cell phones, iPods, or other handheld devices.

Students are prohibited from using Peirce College Technology or Electronic Communications Resources to disparage, ridicule, or denigrate any person or group on the basis of age, sex, race, color, religion, creed, national origin, ancestry, citizenship, disability, sexual orientation, gender identity, marital status, veteran’s status, military status, or membership in any other group protected under local, state, or federal law or to access, post, download, transmit, copy, or
III. ACCEPTABLE USAGE OF COMPUTER SYSTEMS AND FACILITIES

Students are prohibited from using Peirce College Technology or Electronic Communications Resources to send or post messages that contain abusive or objectionable language, that defame or libel others, or that infringe the privacy rights of others. Students shall not view, download, copy, send, post, or access information that is illegal, obscene, or otherwise inconsistent with the College’s nondiscrimination policy or policy prohibiting harassment (for example, sexual images, sexist comments, racist messages, ethnic slurs, and religious slurs).

Students shall not broadcast unsolicited messages, send unwanted mail, make harassing telephone calls, or send chain letters using Peirce College Technology or Electronic Communications Resources.

Students are prohibited from using Peirce College Technology or Electronic Communications Resources to access, archive, distribute, edit, or record adult-oriented websites or sexually explicit or suggestive materials.

Students are prohibited from using Peirce College Technology or Electronic Communications Resources for personal or commercial profit. Examples include, but are not limited to, selling access to your User Login or to Peirce’s systems or networks and using Peirce’s resources to run a personal business.

Students are prohibited from engaging in any other activity that does not comply with the general principles presented above. When in doubt as to whether an activity is prohibited, students should contact their faculty member or the Dean of Students.

Monitoring and Violations
Peirce College will seek to maintain system security and integrity, but students should not assume that their information in their accounts or on Peirce College Technology or Electronic Communications Resources they use is private. The College may access, inspect, search, block, monitor, review, record, archive, and/or disclose any usage conducted through information stored on or information transmitted through Peirce College Technology as well as Electronic Communications Resources, both in real time and after the fact, whether conducted at the College or remotely. In addition, the College reserves the right to access, inspect, search, block, monitor, review, record, archive, and/or disclose any files or other information created, stored, received, or transmitted through College computer or activity on network accounts. By using Peirce College Technology and Electronic Communications Resources, you hereby consent to the foregoing and waive any right to privacy in connection with the activities described in this policy.

Any violations of this policy will result in appropriate corrective and/or disciplinary action. For related information, please refer to the Code of Student Conduct and Responsibility policy, which appears in SECTION I of this Handbook.

The College reserves the right to seek compensation and/or indemnification from a student for damage(s) arising from violations of this policy. In addition, the College and/or third parties may pursue criminal and/or civil action for violations of law.

STUDENT EMAIL
Peirce College provides all students with an email address to facilitate communications between students and the College. When using email to contact Peirce faculty or staff, students are required to use the College-supplied email address.

The College will send all official email communications to students’ College-supplied email address. Students are responsible for reviewing their email at their assigned email address on a frequent and consistent basis. Students should be aware that some email communications are time sensitive. Failure to review email in a timely manner does not
III. ACCEPTABLE USAGE OF COMPUTER SYSTEMS AND FACILITIES

absolve students from complying with the content of such communications.

Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of email, including use for sensitive or confidential information, will be consistent with FERPA. For this reason, Peirce will not and cannot respond to any email from a student not using the official College-supplied email address.

To ensure confidentiality, some private information may be made available only through my.peirce.edu, which is password protected. In these cases, students will receive email correspondence directing them to my.peirce.edu, where they can access their confidential information. The confidential information will not be available in the email message.

For more information, please refer to the FERPA policy, which appears in SECTION VII of this Handbook.

STUDENT VERIFICATION

Peirce College uses a system of secure logins and passwords to ensure that students registering for the course are the students who participate and receive credit.

- Peirce requires that students use a login/password to access their online classes. The password must be reset every 90 days.
- There are no high-stakes exams in Peirce courses that comprise the majority of the grade.
- There are multiple means of assessments in courses, including discussions, projects, papers, quizzes, and exams.

These three, taken together, ensure that the person who is getting credit for the course is in fact the person who has enrolled.

In accordance with the Acceptable Usage of Computer Systems and Facilities, Academic Honesty, and Code of Student Conduct and Responsibility policies, students are responsible for keeping their logins and passwords secure, and upholding the integrity of their coursework. This practice assists the College in protecting students’ privacy and in ensuring that grades are awarded to the appropriate students. Students should immediately report any misuse of student information to the Dean of Students.

PRINTING

Effective September 1, 2011, students will be provided a printing account that will allow them to manage their printing needs at student accessible printers located throughout the College. Student IDs are required to release print requests.

The use of the College owned, leased, or managed equipment and supplies by students is intended for academic purposes. Therefore, students are expected to use discretion when printing materials.

Printer locations:
- Library
- Walker Center for Academic Excellence
- Student Print pods (College Hall 3rd, 5th, & 6th floors)