POLICY – Information and Technology Acceptable Use

Effective: October 2020	**Revision Date(s):**
Questions or Inquiries: Information Technology Department	

Purpose:

All members of the Peirce College community are expected to use the College's information and technology assets according to this policy. This policy applies to all members of the Peirce community, which includes employees, students, visitors, third parties, contractors, consultants, clients, temporaries and others (collectively known as "users"), who have access to, support, administer, manager, or maintain Peirce information and technology assets

Background, Scope and Audience

This policy defines the acceptable use of Peirce College information and technology assets. Those users who violate this policy are subject to the full range of sanctions set forth in the Code of Ethics Policy as well as any applicable local, state and federal laws. This policy may be modified by Peirce at any time without notice to users.

Information security and data privacy requires participation and support from every member of the Peirce community who has access to College systems and data. It is the responsibility of every member of the Peirce community to help ensure the confidentiality, integrity, and availability of all information and technology assets.

In support of its mission of teaching, Peirce provides access to a wide variety of information and technology assets for its users. Access to these information and technology assets is a privilege granted to members of the Peirce community and is vital to performing their daily tasks. Therefore, proper use and protection of Peirce's information and technology assets is essential to the operation of the College.

It is each user's responsibility and obligation to ensure that all information and technology assets are used only for their intended purpose and that information contained or transmitted via these resources is protected from unauthorized access, modification, or destruction. Peirce also recognizes that local, state and federal law relating to copyright, information security and intellectual property are applicable to all members of the Peirce community. The College reserves the right to limit or restrict computing privileges and access to its information and technology assets.

User Responsibility: Those who use Peirce's information and technology assets must act responsibly. Every user is responsible for the integrity of these resources. All users must respect the rights of other users, respect the integrity of the system controls, and maintain the confidentiality of information.

Peirce information and technology assets are provided to an employee to be used for college business only. This applies when the employee is working on campus or working remotely. Specific to working remotely, Peirce assets are loaned to employees so they can conduct college business from a remote location. Those assets remain College property, may not be used by anyone else, and may not be used for personal purposes. This is strictly enforced. There should be no expectation of privacy.

Under no circumstances shall these resources be used to:

- process, transmit, or store data that is unrelated to College business
- distribute copyrighted materials whether it is images, music, software, movies, electronic books, journals, or any other digital content for which the user does not have appropriate rights
- offer goods or services of a commercial nature not sanctioned by the College, such as a private business enterprise

- engage in conduct which is malicious, obscene, threatening or intimidating or which may constitute harassment or bullying
- store College data on any personal storage device, including cloud storage platforms, CD/DVD burners, or any other type of personal removable external storage device or cloud storage services

Employees are not authorized to procure equipment, software, licenses or services on their own. All purchases must be made by the Peirce College Information Technology department.

Electronic Mail (email) and Electronic Messaging (chat): All Peirce email accounts and all data transferred or stored using Peirce email capabilities are the property of the College. As such, email messages are considered part of the College's records and are subject to review, monitoring, auditing and discovery. Therefore, when composing email messages, users must comply with all policies regarding the acceptable use of Peirce's information and technology assets.

Peirce email addresses are not to be used to create or sign into any third-party cloud services that have not been provisioned by the College. Members of the community should use a personal email account to interact with services such as social media or online shopping unless these services are being used exclusively for work being performed on behalf of the College. Email retention is limited to 1 year.

Email older than 1 year will be automatically deleted from email accounts.

Inappropriate Use of Email or other Electronic Messaging (chat): Any inappropriate email, as defined below, is prohibited. Users receiving such email should immediately contact the IT Service Center at servicecenter@peirce.edu. Examples of inappropriate use of electronic messaging include:

- Creating and exchanging messages which are harassing, obscene, or threatening
- Creating and exchanging advertisements, solicitations, or chain letters
- Knowingly transmitting a message containing a computer virus or a message which is intended to trick or mislead the recipient into performing an action
- Misrepresenting the identity of the sender of a message
- Using or attempting to use the accounts of others without their permission
- Unauthorized transmission of College data
- Transmitting Confidential data as defined in the Data Classification Policy
- Transmitting information that is unrelated to College business

Internet Use: Internet access is made available to members of the Peirce community to conduct College business. Users must be familiar with the risks associated with accessing the Internet, including the lack of confidentiality or integrity of information accessed or sent via the internet. Users must be aware that accessing the Internet through the College's network does not afford expanded privacy protections, and that web site operators or other third parties routinely collect and share information about their visitors.

Users must use discretion when posting information using College email addresses on public Internet sites or through social media. Users must observe the protections outlined by the Colleges Data Classification Policy before using any internet service to transmit, store or process Sensitive or Confidential College data.

Network Admission Control and &Anti-Virus Software: As part of Peirce College's ongoing effort to deliver the most reliable network services network, the College reserve the right to determine the information security health of any non-College owned or non-College managed systems that connect to the College network, and to require a baseline level of security, including up-to-date operating system patches, anti-virus/anti-malware software, and/or other requirements before granting access to the College network. This may include a security scan to determine the security posture of your device before being granted access. You are responsible for the state and behavior of your personally owned devices while they are used at Peirce College. Accordingly, every member of the College community and their guest have agreed not to use the network in any way that diminishes the effectiveness of the network or interferes with the reasonable use of those systems by others. Any device that adversely affects the College network or attempts to circumvent College security measures will be isolated from the network without advance notice.

Conflicting Network Services: Users may not connect systems to the College network which emulate, spoof, replicate, or interfere with existing information technology services provided by the College. Prohibited systems include but are not limited to DHCP servers, DNS servers, and wireless access points/personal hot spots. Peirce reserves the right to disconnect without waring any systems which are found to interfering with the ability of other members of the community to connect to or use information and technology resources provided by the College.

Privacy: There should be no expectation of privacy when using the College's information technology assets.

The College may monitor transmissions should a violation of this policy be alleged or in the course of performing routine maintenance or troubleshooting a problem. System administrators or other authorized personnel may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged.

Any file may be subject to search by law enforcement agencies under court order, if such a file contain information which may be used as evidence in a court of law. Information Technology staff may access college-owned computers to perform system maintenance either on-site or using remote tools as necessary without prior notification.