PIERPONT COMMUNITY & TECHNICAL COLLEGE
Board of Governors Policies and Procedures
POLICY # 53
TITLE: INFORMATION TECHNOLOGY

Effective Date: October 24, 2007
Amended: October 20, 2015
Repealed:

SECTION 1: SCOPE

1.1 This policy establishes a base line for Pierpont Community & Technical College's expectations of our user community. It applies to all users of the Fairmont State Information Technology Environment (**FSITE**), including all faculty, staff, students, contractors, consultants, temporaries, as well as those who represent themselves as being connected in any way with Pierpont and/or who make use of Pierpont computing and/or information technology (IT) resources. All FSITE users are expected to be familiar with and comply with this policy. Violations of policies governing the use of FSITE may result in restriction of access to Pierpont information technology resources in addition to any disciplinary action that may be applicable under other Pierpont policies, guidelines, or procedures, up to and including dismissal.

1.2 Use of any FSITE resource implies consent to the Information Technology Policy at Pierpont Community & Technical College.

SECTION 2: DEFINITIONS

2.1 The FSITE includes but is not limited to all personal computers connected to "the network" on any Pierpont campus or which utilize any Fairmont State technological resource from any destination worldwide.

2.2 Unified Computer Account (UCA) is the username to log in to Pierpont computer systems.

SECTION 3: ACCEPTABLE USE

3.1 The basic premise of this policy is that responsible and acceptable use of FSITE does not extend to whatever an individual is technologically capable of doing. Instead, certain principles provide a guide to users regarding responsible and acceptable behaviors and users are responsible for knowing and understanding them. These principles and guidelines include, but are not limited to:

3.1.1 Authorized users of FSITE or Pierpont sponsored resources are those individuals who have been granted a UCA and password. The UCA and password combination is an individual's identity and license to access and use the components of FSITE for which they are specifically authorized.

3.1.2 Authorized users will abide by institutional policies along with applicable local, state and federal laws or regulations.

3.1.3 The resources of FSITE are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. The FSITE may NOT be used for commercial or profit-making purposes.

3.1.4 Pierpont reserves the right to limit access to the FSITE when investigating cases of suspected abuse or when violations have occurred.

3.1.5 The College does not monitor or generally restrict the content of material stored on or transferred through the components of the FSITE. However, use of the FSITE is intended for work-related purposes and not to serve as a public forum. Pierpont reserves the right to restrict or deny usage of the FSITE in those situations where it is determined that a specific usage is not work-related or supportive of the institution's mission or does not abide by institutional policies, local, state and federal laws or regulations.

3.1.6 Users must adhere to the ethical standards governing copyright, software licensing, and intellectual property.

3.2 Individuals using FSITE resources and services must be identified through an authorized UCA. In the case of multiple user systems, individuals may not knowingly access or use another person's UCA or knowingly allow another person to use his or her UCA. Users should log out of shared systems and take reasonable precautions to secure access to office computers. The FSITE and services may not be used intentionally to misuse or gain unauthorized access to another user's UCA or systems inside or outside of the FSITE.

3.3 Computer users may use only legally obtained, licensed data or software in compliance with Pierpont copyright policies as well as license or other agreements and applicable copyright or intellectual property laws. Pierpont is a member of EDUCAUSE and users are expected to adhere to the Code of Software and Intellectual Rights which states, "Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community. (See: "Using Software: A Guide to the Legal and Ethical Use of Software for Members of the Academic Community," Educom/ITAA, 1992. http://www.educause.edu/ir/library/html/code.html)"

3.4 Users of the FSITE must respect the privacy of others by refraining from inspecting, broadcasting, or modifying data without the consent of the individual or individuals involved, except as permitted as part of their employment or educational requirements, and then only to the extent necessary. Members of the Pierpont community may not seek out, examine, use, modify, or disclose, without authorization, personal or confidential information which they need not access as part of their campus function. All faculty members, staff, students and other Pierpont community members must take necessary precautions to protect the confidentiality of personal and/or confidential information available to them

3.5 Users of Pierpont e-mail or other electronic communications shall not employ a false identity, nor send e-mail anonymously with the intent to deceive or harass.

3.6 The FSITE shall not be used for purposes that cause, or could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted/unsolicited interference with others' use of computing systems and services.

3.6.1 This provision explicitly prohibits the posting of unsolicited electronic mail to lists of individuals, and the inclusion on electronic mail lists of individuals who have not requested membership on the lists. Students will automatically be members in an electronic mailing list for a class in which they are registered or for the purpose of official communications between authorized Pierpont personnel and an identified group of students. Faculty and staff are required to accept membership in an electronic mailing list for the purpose of official Pierpont communications, which are not prohibited.

3.6.2 Alumni and other individuals affiliated with, but not employed by, the university may be included in electronic mail lists, but may opt out by request to the sender.

3.6.3 Marketing emails for Institutional use is excluded from this provision, provided all required State and Federal guidelines pertaining to mass emailing are followed.

3.7 FSITE resources and services may not be used in an obscene, harassing or otherwise inappropriate manner. University computing systems will not be used to unlawfully discriminate against any person on the basis of race, color, religion, sex, national origin, age, disability, veteran status, or sexual orientation. Any sexually explicit or pornographic material may NOT be viewed, obtained or sent from any computer connected to the FSITE unless it is being done so for an acceptable academic purpose. Should there be a question as to appropriate use of sexually explicit or pornographic material for academic purposes, final determination will be made by the Vice President for Academic Affairs.

SECTION 4: E-MAIL

4.1 Eligibility

A Pierpont UCA provides access to a number of information systems, including Google Apps for Education, Pierpont's e-mail system. All individuals and organizations with a Pierpont UCA are eligible to receive a Pierpont e-mail account. In order to keep a Pierpont e-mail account, the group or individual must maintain eligibility for a Pierpont UCA account. UCA accounts may be termed "inactive" or "purged", in which case access to the email system would be revoked and, in the case of "purged" accounts, all e-mail irrevocably deleted.

4.1.1 A UCA may be determined "inactive" if it goes unused for a period of 12 months.

4.2 Requirements

All eligible faculty, staff and students must create and maintain a Pierpont e-mail account. Contractors to Pierpont may be required to have and maintain an account as well. This is required to facilitate Pierpont's communication of academic, administrative and emergency information. Exceptions may be made for employees without regular access to computing resources. It is permissible to forward mail from the Pierpont account to another email account as long as that account is checked regularly. However, it is not advisable to do so, since e-mail communications may contain sensitive information that should not be transmitted out of Pierpont systems.

4.3 Maximum Message Size

Outgoing and incoming e-mails may be limited in size, including the text and all attachments. Messages over the limit will not be delivered or received, and users will be informed that their

message was not delivered or received. The limit includes the extra space to allow for overhead space that is taken up when sending attachments.

4.4 Unsolicited and Mass E-mail and LISTSERVS

Mass e-mails should only be used to communicate Pierpont sponsored activities, security alerts, policy changes, or information that benefits Pierpont business or academic missions. Mass e-mails should relay time-critical, important Pierpont information and should be used sparingly.

4.4.1 There are recommended limitations for Mass Email Interface Users, and overuse can lead to suspension of access. Users must also follow guidelines for Email content as defined below in the Email Message section.

4.4.2 Users are not permitted to spam using Pierpont's e-mail service.

4.4.3 Standard email groups are maintained by IT and are available for all Faculty and Staff to utilize. Custom email groups can be created by individuals within their account.

4.4.4 The Pierpont email system and the email groups within are for official use only.

4.5 Backups

The Pierpont email system is backed up 3 times per day, with a full or incremental backup. Each night's backup is kept for 10 days. These backups may be used for disaster recovery and policy compliance purposes.

4.6 Virus Protection

The Google Apps system has a virus scanner that scans all incoming and outgoing e-mail for viruses, and removes them when found. However, this virus scanner cannot guarantee that all e-mail will be virus-free. Thus, all e-mail users should have their own anti-virus software on their computers. Anti-virus software is available at no charge to members of the Pierpont community via the IT Department. Pierpont is not liable for any damage caused by viruses or any other hostile code delivered through the email system.

4.7 Inappropriate Usage

E-mail users should only use the e-mail services in an appropriate manner. Inappropriate usage may result in revocation of access to Pierpont email. Inappropriate usage includes, but is not limited to:

- Unauthorized attempts to access another's e-mail account
- Transmission of sensitive or proprietary information to unauthorized persons or organizations
- Transmission of obscene or harassing messages to any individual(s)
- Transmission of copyrighted materials in violation of the rights of the copyright holder
- Solicitation for personal or private gain.
- Any illegal or unethical activity or any activity that could adversely affect Pierpont

4.8 Privacy and Applicability of Laws and Policies

This policy clarifies the applicability of law and certain other Pierpont policies to electronic mail. Users are reminded that all usage of Pierpont's information technology resources, including electronic mail, is subject to all Pierpont policies. Pierpont encourages the use of electronic mail and respects the privacy of users. It does not wish to inspect or monitor electronic mail routinely or to be the arbiter of its contents. Nonetheless, electronic mail and data stored on the Pierpont's network of computers and servers may be accessed by the Office of Information Technology for the following purposes:

- Troubleshooting hardware and software problems
- Preventing unauthorized access and system misuse
- Retrieving business related information
- Investigating reports of violation of Pierpont policy or local, state or federal law
- Complying with legal requests for information
- Rerouting or disposing of undeliverable mail
- Other purposes deemed necessary by the Office of Information Technology with the approval of the Chief Information Officer and the President.

4.8.1 The system administrator will need approval from the Chief Information Officer (or someone designated by the CIO), and the President's Office to access specific mail and data for these purposes. The extent of the access will be limited to what is reasonably necessary to acquire the information.

4.8.2 The Office of Information Technology may also retrieve electronic mail messages delivered to Pierpont account holders, or otherwise prevent distribution of a message to Pierpont e-mail accounts, if it is determined that distribution of the message(s) violates local or federal law, Pierpont policy, or places Pierpont at risk of violation of privacy-related laws. The system administrator will need approval from the CIO (or someone designated by the CIO), to retrieve specific mail messages, and the extent of the access will be limited to what is reasonably necessary to retrieve the information.

4.8.3 Individuals' privacy should be preserved. However, there is no expectation of privacy or confidentiality for documents and messages stored on institutionally-owned equipment or systems. Users of electronic mail systems should be aware that in addition to being subject to authorized access, electronic mail in its present form cannot be secured and is vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the purported sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents.

4.8.4 Users of electronic mail services should be aware that even if the sender and recipient have discarded their copies of an electronic mail record, there might be back-up copies of such electronic mail that can be retrieved.

4.8.5 Pierpont electronic mail services may, subject to the above, be used for incidental personal purposes provided such use does not interfere with Pierpont operation of information technologies or electronic mail services, burden Pierpont with incremental costs, or interfere with the user's employment or other obligations to Pierpont. Electronic mail may constitute a public record like other documents subject to disclosure as a result of litigation.

4.9 Liability

Pierpont provides e-mail service to facilitate the sending and receiving of e-mail within the Pierpont community and to the world. The Office of Information Technology makes all reasonable effort to ensure that e-mail is sent, received, and stored appropriately. However, the Office of Information Technology provides no assurances that e-mail will be sent or received using the system, and cannot be held liable for missing messages or any consequences of that message not being sent, delivered, or stored.

4.9.1 Pierpont acts as a common carrier of e-mail messages, and does not examine the content of e-mail messages, except as noted above. As such, Pierpont cannot be held liable for the content of any e-mail message sent, received, or stored on the Pierpont system, or for any consequences of that message being sent, delivered, or stored. Pierpont is also not liable for any damage caused by viruses or other hostile code delivered through the Pierpont email system.

SECTION 5: WEB CONTENT

5.1 The content of all pages must adhere to Pierpont policies and be incompliance with the institution's Copyright and Privacy policies and local, state and federal laws.

5.2 None of the pages located on Pierpont servers can be used to promote personal financial activity, commercial activity, non-profit organizations not directly affiliated with Pierpont, political groups or religious groups, unless permitted by other College policy or regulation.

SECTION 6: ENFORCEMENT

6.1 Computer activity may be monitored by authorized individuals for purposes of maintaining system performance and security. In instances when individuals are suspected of abuse of the FSITE, the contents of user files may also be inspected upon the approval of the Office of Information Technology or someone designated by the CIO.

6.2 Violations of Pierpont policies governing the use of the FSITE may result in restriction or termination of access to FSITE systems and resources or termination of employment or expulsion. In addition, disciplinary action may be applicable under other Pierpont policies, guidelines, procedures, or collective bargaining agreements, up to and including imprisonment. At the discretion of the manager of the computer system or service in question, or designee, in collaboration with the appropriate authority, computer use privileges may be temporarily or permanently revoked pending the outcome of an investigation of misuse, or finding of violation of this rule. Where practical and appropriate, 24-hour notice will be given in advance of revocation.

6.3 All data, programs, and files placed on or contained in the FSITE computer systems are subject to Pierpont's copyright, patent, and privacy policies. Additional rules may be in effect at specific computer facilities at the discretion of the directors of those facilities.