PASCO-HERNANDO STATE COLLEGE

INTERNAL MANAGEMENT MEMORANDUM #1-19

TO: **All Faculty and Staff**

FROM: **Katherine M. Johnson, President**

DATE: **May 4, 2009**

SUBJECT: **Acceptable Use of College Technology Resources**

The purpose of this Internal Management Memorandum (IMM) is to establish the conditions and guidelines for the use of College technology resources including hardware, software, the College network, and peripherals such as printers and scanners.

Pasco-Hernando State College (PHSC) is committed to providing access to technology for faculty, staff, and students as a means of enhancing its educational mission.

PHSC makes no warranties of any kind, whether expressed or implied, for the use of College-owned computer equipment. The College will not be responsible for any damages such as loss of data resulting from service interruptions, hardware or software failure, or viruses. The computer systems including hardware, software, and network equipment are the sole property of the College. These systems may be used only for lawful purposes. The use of College-owned equipment is at the risk of the user. PHSC property may be used only for College-related activities.

Effective security is a team effort involving the participation and support of every PHSC employee and student who deals with information and/or information systems. All faculty and staff are provided with a unique ID for access to the College personal computers and College network. They are required to utilize and keep secure their passwords for all systems to which they have authorized access. They are required to use due diligence in protecting all confidential or personal information to which they may have access. It is the responsibility of every computer user to know these guidelines

To protect the college technology, all installation or removal of software or hardware on College systems, will be performed by the following PHSC personnel:

a. Network staff;
b. MIS staff;

c. Other College personnel who have been properly trained by the Network Department and have written permission of the Network Department for each software program to be installed;
d. Vendors in fulfillment of a contracted service; or
e. Students enrolled only in the following classes: A+Certification, Cisco Academy courses, Networking Services program, and Information Security program for the course related technology.

General Use and Ownership

While PHSC desires to provide a reasonable level of privacy, users should be aware that the data they create on the school's systems remains the property of Pasco-Hernando State College. Because of the need to protect Pasco-Hernando State College's network, staff cannot guarantee the confidentiality of information stored on any network device belonging to Pasco-Hernando State College.

Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 20 minutes or less, or by logging-off when the host will be unattended.
3. Because information contained on portable devices is especially vulnerable, special care should be exercised. No sensitive, confidential, or personally identifiable information will be kept on any portable storage devices including laptops, PDAs, CD/DVD, flash drives unless the data is encrypted. Pasco-Hernando State College is not responsible for any damage to a users' personal software or hardware.
4. Postings/emails by users to forums or emails to other students, staff, or faculty or to the public should not contain inappropriate material/content including sensitive, confidential, or personally identifiable information. User privileges can be denied to anyone who misuses College systems/software.

Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Pasco-Hernando State College-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Pasco-Hernando State College.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Pasco-Hernando State College or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Pasco-Hernando State College computing asset to actively engage in procuring or transmitting material that constitutes sexual harassment or creates a hostile environment based on race, gender, or other protected classifications.
7. Making fraudulent offers of products, items, or services originating from any Pasco-Hernando State College account.
8. Buying or selling weapons or illegal substances via Pasco-Hernando State College's technology (i.e. hardware and/or software.)
9. Threatening or "stalking" or harassing others through the use of Pasco-Hernando State College's technology.
10. Trafficking in pornography of any kind via Pasco-Hernando State College's network. Please note that redistribution of pornography, even through web page links, is often illegal.
11. Activities that violates state or federal law. This may include viewing, downloading, posting, printing or sending pornography, or other sexually explicit, profane, obscene, hostile, or blatantly offensive and intimidating material, including hate speech, threats, harassing communications (as defined by law), or information that violate any state or federal laws.

12. "Spam", the practice of indiscriminately sending unsolicited email (e.g., commercial advertisements, chain mail, pornographic materials, political

lobbying, hate speech, racial diatribes, and religious proselytizing) to persons who have not indicated interest in receiving such materials.

13. “Hacking” or “Cracking”, i.e., deliberately invading the privacy of others by attempting to gain unauthorized access to any account or system.
14. Obtaining/distributing confidential information. Deliberately and inappropriately observing, recording, accessing, using or transmitting passwords, account numbers, email addresses, phone numbers, or credit card numbers belonging to other people is prohibited.
15. Downloading executable programs, which might interject computer viruses into lab computers, is generally prohibited. Further guidance with regard to safe sites and appropriate downloads should be sought from the lab facilitator. (PHSC takes no responsibility for damage to your work or your own equipment resulting from viruses or files you might download via the Internet).
16. Using Pasco-Hernando State College’s equipment, including the College’s Internet lines, servers or web pages, for commercial gain.
17. Unauthorized wiring, altering or damaging of Pasco-Hernando State College-owned computer equipment, including hardware and software.
18. Tampering with machine settings of any Pasco-Hernando State College computer.
19. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
20. Port scanning or security scanning is expressly prohibited.
21. Executing any form of network monitoring which will intercept data not intended for the user's host.
22. Circumventing user authentication or security of any host, network or account.
23. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

E-mail and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, instant messaging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Pasco-Hernando State College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Pasco-Hernando State College or connected via Pasco-Hernando State College's network.

The College reserves the right to bypass individual student and employee passwords at any time and to monitor the use of such systems by students and employees. The use of College-owned computer resources is a privilege, not a right. Any violation of the regulations above is unethical and may constitute a criminal offense. Breaches of this policy may result in College disciplinary action and/or appropriate legal action.

Under no circumstances is anyone authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PHSC technology resources.

Violation of these procedures will be handled in accordance with the procedures outlined in the *College Catalog/Student Handbook* and the *Personnel Manual.*

KMJ/scs

History: 08/01/99 (new)
08/02/99
06/12/00
06/17/02
06/30/03
06/06/05
08/01/05
02/16/09