

ADMINISTRATIVE PROCEDURES

Title: ACCEPTABLE USE	Identification:	9.00
	Page:	1 of 5
	Effective Date:	March 26, 2013
Authority: SBE 6A-14.0261 FS 1001.64; 1001.65	Signature/Approval:	Dr. Ken Atwater

PURPOSE

This procedure establishes and outlines the Acceptability Standards to which authorized users may access technology resources at Hillsborough Community College.

PROCEDURE

1. ACCESS

Access to HCC's information technology resources is a privilege granted to HCC users (faculty, staff and students) in support of their studies, instruction, duties as employees, official business with the College, and/or other College-sanctioned activities. Access may also be granted to individuals outside of HCC for purposes consistent with the mission of the College.

With the exception of publicly accessible resources such as websites, access to HCC information technology resources may not be transferred or extended by members of the College community to outside individuals or groups without prior approval of the Vice President of Information Systems or his/her designee. Such access must be limited in nature and fall within the scope of the educational mission of the institution.

Gaining access to the College's information technology resources does not imply the right to use those resources. The College reserves the right to limit, restrict, remove or extend access to and privileges within, material posted on, or communications via its information technology resources, consistent with this procedure, applicable law or as the result of College disciplinary processes, and irrespective of the originating access point.

It is expected that these resources will be used efficiently and responsibly in support of the mission of the College as set forth in this procedure. All other use not consistent with this procedure may be considered unauthorized use.

2. DATA SECURITY, CONFIDENTIALITY AND PRIVACY

HCC users are responsible for ensuring the confidentiality and appropriate use of institutional data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students, faculty and staff concerning the use and release of personal information, as required by Florida Statutes, Federal Laws or existing policies (i.e. Chapter 815, Florida Statutes, Computer Crimes Act, Title 18, United States Code, Electronic Communications Privacy Act of 1986, Gramm-Leach-Bliley Act, Family Educational Right to Privacy Act, etc.)

Electronic mail and computer files are considered private to the fullest extent permitted by law. Access to such files will generally require permission of the sender/recipient of a

message or the owner of the account in which the material resides, court order, or other

ADMINISTRATIVE PROCEDURES

Identification: 9.00	Page: 2 of 5	Effective Date: March 26, 2013
---------------------------------------	-------------------------------	---

actions defined by law, College policy or procedure. However, in the event of a College investigation for alleged misconduct, e-mail or files may be locked or copied to prevent destruction and loss of information.

All users of HCC's information technology resources are advised to consider the open nature of information disseminated electronically, and they should not assume any degree of privacy or restricted access to such information. HCC strives to provide the highest degree of security when transferring data, but the College cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

3. **ELECTRONIC INFORMATION RETENTION AND DISCLOSURE**

Original electronic materials on central computing equipment and/or copies may be retained for specified periods of time on system backups and other locations; however, the College does not warrant that such information can be retrieved.

Electronic files or messages, whether or not created and stored on College resources, may constitute a College record subject to disclosure under the Florida Public Records Act or other laws, or as a result of litigation. Electronic copies must be provided in response to a public record request or legally issued subpoena, subject to very limited exceptions, as with other documents created and retained by the College.

Disclosure of confidential information to unauthorized persons or entities, or the use of such information for self-interest or advantage, is prohibited. Access to non-public institutional data by unauthorized persons or entities is prohibited.

Requests for disclosure of confidential information and retention of potential evidence will be honored when approved by authorized College officials or required by state or federal law.

4. **NETWORK AND SYSTEM INTEGRITY**

In accordance with Florida Statutes and other policies and laws, activities and behaviors that threaten the integrity of computer networks or systems are prohibited on both College-owned and privately-owned equipment operated on or through College resources. These activities and behaviors include, but are not limited to:

- a. Intentional or careless interference with or disruption of computer systems and networks and related services, including but not limited to the propagation of computer "worms," "viruses" and "Trojan Horses" and other activities that could have a negative impact on the HCC computing environment in the judgment of the Vice President of Information Systems or designee.
- b. Intentionally or carelessly performing an act that places an excessive load on a computer or network to the extent that other users may be denied service or the use of electronic networks or information systems may be disrupted

ADMINISTRATIVE PROCEDURES

Identification: 9.00	Page: 3 of 5	Effective Date: March 26, 2013
--------------------------------	------------------------	--

- c. Failure to comply with authorized requests from designated College officials to discontinue activities that threaten the operation or integrity of computers, systems or networks
- d. Negligently or intentionally revealing passwords or otherwise permitting the use by others of College-assigned accounts for computer and network access. Individual password security is the responsibility of each user. The user is responsible for all uses of their accounts, independent of authorization.
- e. Altering or attempting to alter files or systems without authorization
- f. Unauthorized scanning of ports, computers and networks
- g. Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities
- h. Connecting unauthorized equipment to the campus network or computers.
- i. Attempting to alter any College computing or network components, including but not limited to bridges, routers, hubs, wiring, and connections, without authorization.
- j. Utilizing network or system identification numbers or names that are not assigned for one's specific use on the designated system
- k. Using campus resources to gain unauthorized access to any computer system and/or using someone else's computer without permission
- l. Registering a HCC IP address without permission from the Vice President, Information Systems.

5. **COMMERCIAL USE**

Use of the College's information technology resources is strictly prohibited for unauthorized commercial activities, personal gain, and private, or otherwise unrelated to the College business. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling College resources.

6. **FRAUD**

Use of College information technology resources for purposes of perpetrating fraud in any form is strictly prohibited. Fraudulent activities include but are not limited to sending any fraudulent electronic transmission, fraudulent requests for confidential information and fraudulent submission and/or authorization of electronic purchase requisitions.

ADMINISTRATIVE PROCEDURES

Identification: 9.00	Page: 4 of 5	Effective Date: March 26, 2013
--------------------------------	------------------------	--

7. **HARASSMENT**

Harassment of others via electronic methods is prohibited under Florida Statutes and other applicable laws and College policies or procedures. It is a violation of this procedure to use electronic means to harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference.

8. **COPYRIGHT AND FAIR USE**

Federal copyright law applies to all forms of information, including electronic communications, and violations are prohibited. Infringements of copyright laws include, but are not limited to, making unauthorized copies of any copyrighted material (including software, computer code, text, images, audio, and video), and displaying or distributing copyrighted materials over computer networks without the author's permission except as provided in limited form by copyright fair use restrictions. The "fair use" provision of the copyright law allows for limited reproduction and distribution of published works without permission for such purposes as criticism, news reporting, teaching (including multiple copies for classroom use), scholarship, or research. The College will not tolerate academic dishonesty or theft of intellectual property in any form.

9. **ELECTRONIC COMMUNICATIONS**

College electronic communications are to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences, to facilitate the effective business and administrative processes of the College, and to foster effective communications within the academic community. Electronic mail, news posts, chat sessions or any other form of electronic communication must comply with Florida Statutes, Florida Educational Code, HCC Policies and Procedures and the Student Code of Conduct.

10. **WEBSITES**

An official HCC web page is one that is formally acknowledged by the chief officer of a College department or division as representing that entity accurately and in a manner consistent with HCC's mission: Without such acknowledgment, a website, regardless of content, is not "official." Official pages are the property and responsibility of the College or department that created them and follow the College Web Style Guide and College Logo Guidelines "Unofficial" information may also be posted and maintained by individual faculty, staff and student organizations. HCC does not undertake to edit, screen, monitor, or censor information posted by unofficial authors, whether or not originated by unofficial authors or third parties, and does not accept any responsibility or liability for such information even when it is conveyed through College-owned servers.

Web sites are subject to the other provisions of this procedure if they use College resources such as College-owned servers and the HCC network to transmit and receive information.

ADMINISTRATIVE PROCEDURES

Identification: 9.00	Page: 5 of 5	Effective Date: March 26, 2013
--------------------------------	------------------------	--

11. **POLICY COMPLIANCE**

The Vice President of Information Technology or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate College officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

The Vice President of Information Technology or designee will inform users about the procedure; receive and respond to complaints; collect and secure evidence as required; advise and assist College offices on the interpretation, investigation and enforcement of this policy; consult with College Legal Counsel on matters involving interpretation of law, campus policy, or requests from outside law enforcement agencies and/or legal counsel; and maintain a record of each incident and its resolution to inform future policy changes.

12. **CONSEQUENCES OF NON-COMPLIANCE**

Non-compliance may lead to College disciplinary action under College disciplinary policies and procedures for students and employees, private civil action, and/or criminal charges.

13. **REPORTING IRRESPONSIBLE OR INAPPROPRIATE USE**

The Vice President of Information Technology or designee is responsible for reviewing violations of this procedure and will act in accordance with College policies, procedures and guidelines for investigations and resolution of problems. Suspected infractions of this procedure should be reported to the Vice President of Information Technology. Any employee may report a violation of this procedure.

HISTORY: New