

## Acceptable Use Policy

### Office of Information Technology

#### Access

Access to HCC's information technology resources is a privilege granted to HCC users (faculty, staff and students) in support of official College business and 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 written prior approval of the appropriate College official. Such access must be limited in nature and fall within the scope of the educational mission of the institution. The authorizing College official is responsible for ensuring that such access is not abused.

Simply 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 or restrict access to its information technology resources due to inappropriate use of these resources based on this policy, applicable state and federal laws and regulations, or as the result of College disciplinary processes. Access may be denied to individuals or systems either inside or outside of the College's network if inappropriate behaviors are detected.

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

All users of HCC computing resources must comply with federal and state laws, HCC rules, policies and procedures, and the terms of applicable contracts including all software licenses when using HCC computing resources. Some examples of applicable laws, rules, college procedures and policies include:

- Libel
- Privacy
- Copyright
- Trade Mark
- Obscenity and Child Pornography
- Florida Computer Crimes Act
- The Electronic Communications Privacy Act
- The Computer Fraud and Abuse Act (prohibiting "hacking" and related actions)
- The HCC Student Code of Conduct
- HCC Sexual Harassment Rule
- HCC IT Operating Procedures

All users who engage in electronic communications with other countries or on other systems and networks may be subject to laws of other jurisdictions and the rules and policies of other networks and systems.

### **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. Users are required to ensure the security of the equipment where confidential information is held or displayed and ensure the security of any accounts issued in their name. All users are required to protect the privacy rights of students, faculty and staff by protecting against the unauthorized release of personal information, as required by Florida Statutes, Federal Statutes, and HCC policies and procedures which include but are not limited to: (i.e. [Chapter 815, Florida Statutes, Computer Crimes Act](#), [Title 18, United States Code Chapter 121](#), [Electronic Communications Privacy Act of 1986](#), [Gramm-Leach-Bliley Act](#), [Family Educational Right to Privacy Act](#)).

However, in the event of a College investigation for alleged misconduct, network access, e-mail, files or equipment assigned to any user may be removed, secured 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 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 cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

### **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 always be retrieved.

HCC reserves the right to delete stored files and messages to preserve system integrity as permitted by Florida law. HCC also reserves the right to modify system parameters provided timely notice is provided to system users when appropriate. Except in an emergency, users will be given advance notice, taking the academic year calendar into account, to save any personal files and messages prior to the deletion of these stored records.

Electronic files or messages stored on College resources, may constitute a public record subject to disclosure under the [Florida Public Records Act](#) (Chapter 119, Florida Statutes) or other state and federal laws. Electronic copies must be provided in response to a public record request or legally issued subpoena or court order, subject to very limited exceptions, as with other documents created and retained by the College. All public records requests must be forwarded to the Executive Director of Marketing and Public Relations.

Disclosure of confidential College 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 require approvals by authorized College officials as required by state or federal laws.

Email created or received by HCC employees in connection with official business which perpetuates, communicates, or formalized knowledge is subject to the public records law and open for inspection. If your email falls within the definition of a public record, you may not delete it except as provided in the HCC and state of Florida Record Retention statute, and you must produce the email to any person on request. A person does not need a legitimate need for public records to inspect them. There are several state and federal exemptions to the Public Records Law:

- Certain documents involving personnel matters are confidential under Florida law;
- Student records, except for directory information must be kept confidential before any email is released pursuant to a Public Records Request, any exempt information must be deleted from the email. All Public Records Requests should be referred to your administrative supervisor.

### **Network and System Integrity**

In accordance with federal and Florida laws, [FIRN \(Florida Information Resource Network\) Acceptable Use Policy](#) and other HCC rules, policies and procedures, activities and behaviors that threaten or interfere in any manner with the integrity of computer networks or systems are prohibited on both College-owned and privately-owned equipment operated on or through College-owned technology resources. These activities and behaviors include, but are not limited to:

1. 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 "Trojans" or other activities that could have a negative impact on the HCC computing environment.
2. 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.
3. Failure to comply with authorized requests from designated College officials to discontinue activities that threaten the operation or integrity of computers, systems or networks.
4. 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.**
5. Altering or attempting to alter files or systems without authorization.
6. Unauthorized scanning of ports, computers and networks.
7. Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities.
8. Connecting unauthorized equipment to the campus network or computers.
9. Attempting to alter any College computing or network components, including but not limited to bridges, routers, hubs, wiring, and connections, without authorization or beyond one's level of authorization as designated by the administrator responsible for that equipment, i.e. the Vice President of Information Technology, or designee.

10. Utilizing network or system identification numbers or names that are not assigned for your specific use on a designated system.
11. Using campus resources to gain unauthorized access to any computer system and/or using someone else's computer without their permission
12. Providing services or accounts on College computers or via College networks to other users, unless required to meet the normal activities of students to fulfill current course requirements.
13. Registering an HCC IP address with any other domain name other than for official College business.
14. Imply or speak on behalf of HCC or use HCC trademarks/logos without prior authorization.

It is recognized that Information Technology programs have unique needs that may require exceptions from the restrictions within this Acceptable Use Policy. Because of these needs an Experimental Network, that is separate from the college-wide network, will be established and exempted from the restrictions of this Acceptable Use Policy except where state and federal laws apply. The Experimental Network will be governed by its own Acceptable Use Policy. Any Experimental Network traffic that passes outside the college firewall will be in compliance with the FIRN Acceptable Use Policy.

### **Commercial Use**

Use of the College's information technology resources for unauthorized commercial activities or fundraising is strictly prohibited. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling College resources.

Campus auxiliary organizations are authorized to provide services and products to students, faculty and staff, and invited guests of the College through their operations. The College President or designee may authorize additional limited commercial uses. Such uses are excluded from the above prohibitions. These prohibitions are not intended to infringe on authorized uses that enable students, staff and faculty to carry out their duties and assignments in support of the College mission.

### **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 purchases.

### **Political Activities:**

Section 104.31, Florida Statutes prohibits the use of state resources for political campaign activity. This provision does not apply to political activities related to on-campus student government, including the conduct of student elections, or student club activities and sponsored events conducted with prior approval of the College President. Such activities must comply with all other provisions of this policy, including the section on electronic communications, when using College resources.

## **Harassment**

Harassment of others via electronic methods is prohibited under [Florida Statutes and other applicable laws](#) and [Administrative Rules](#) and [procedures related to sexual harassment](#). It is a violation of this policy to use electronic means to harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference.

## **Copyright and Fair Use**

[Federal copyright law](#) applies to all forms of information, including electronic communications, and violations are prohibited under this policy. 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 laws](#) 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.

## **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, HCC Administrative Rules, Policies and Procedures, and the Student Code of Conduct.

E-mail and computer files are subject to Florida Public Record Laws with some exceptions. Examples of inappropriate uses of email include but are not limited to:

- Chain letter emails
- Hate email
- Harassing email
- Spamming
- Junk email
- False Identification (spoofing)

Retention periods must be followed for all HCC email as required by the Florida Public Record Retention Law.

## **Web Sites**

An official HCC web page is one that is formally acknowledged by the appropriate departmental administrator as representing that entity accurately and in a manner consistent with HCC's mission and are intended for HCC official business. Without such acknowledgment, a web site, regardless of content, is not "official." Official pages are the property and responsibility of the College and department that created them and must 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. Employee pages represent an employee in his or her primary role as an HCC employee. HCC does not undertake to edit, screen, monitor, or censor information posted by unofficial authors and does not accept any responsibility or liability for such information even when it is conveyed through College-owned servers. Incidental personal information on an employee page is acceptable as long as it does not interfere with the function of a unit, disrupt service, incur costs to HCC, or cause excessive use of resources.

Both official and unofficial web sites are subject to the provisions of this policy if they use College resources such as College-owned servers and the HCC network to transmit and receive information

### **Policy Compliance**

The Vice President of Information Technology, or designee, is authorized by the President to ensure that the appropriate processes to administer the policy are in place, communicated and followed by the College community. The Vice President for 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 processes in accordance with due process.

The Vice President of Information Technology, or designee, will inform users about this policy; 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.

### **Consequences of Non-Compliance**

Enforcement will be based upon receipt by Office of Information Technology of one or more formal complaints about a specific incident or through discovery of a possible violation in the normal course of administering information technology resources.

First offense and minor infractions of this policy, when accidental or unintentional, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the resource in consultation with the Department of Human Resources or the Student Code of Conduct.

Repeated offenses and serious incidents of non-compliance may lead to College disciplinary action under HCC disciplinary policies and procedures for students and employees, employee contract provisions where appropriate, private civil action, and/or criminal charges. Serious incidents of non-compliance include but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, copyright violations, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior and violation of State or Federal statutes.

In addition to the above, inappropriate use of information technology resources may result in personal criminal, or civil penalties.

### **Reporting Irresponsible or Inappropriate Use**

The Vice President of Information Technology, or designee, is responsible for reviewing violations of this policy and will act in accordance with College policies and guidelines for investigations and resolution of problems. All HCC employees must report any infraction to the employee's immediate supervisor who will in turn report it to the Vice President of Information Technology. The supervisor will, in consultation with Human Resources or the Student Code of Conduct (whichever rules are appropriate for the offense) take those actions that are appropriate under this policy and HCC disciplinary procedures.

HCC's Acceptable Use Policy is subject to change so users should periodically review this policy.

Approved: 11/12/2008