

Houston Community College
Guidelines for Security and Acceptable Use

Date: **September 24, 2009**

TABLE of CONTENTS

OVERVIEW.....	1
DEFINITIONS	1
APPLICABILITY.....	1
GUIDELINES	1
ADMINISTRATIVE RESPONSIBILITY.....	1
COMPUTER USAGE	2
RIGHTS & RESPONSIBILITY.....	2
COPYRIGHT & INTELLECTUAL PROPERTY.....	2
SOFTWARE USE	2
DAMAGE OR IMPAIRMENT OF HCC RESOURCES.....	2
UNAUTHORIZED COMMERCIAL ACTIVITIES.....	3
COMPUTER HARASSMENT.....	3
SECURITY	3
ROUTINE LOGGING AND MONITORING.....	3
SEVERABILITY (FACULTY/STAFF)	3
ELECTRONIC MAIL	3
RIGHTS & RESPONSIBILITY.....	3
CONFIDENTIALITY & SECURITY	4
WEB PAGES.....	4
SECURITY	5
PASSWORDS.....	5
VIRTUAL PRIVATE NETWORK (VPN) ACCESS.....	5
ACCESS TO SECURE IT AREAS.....	5
PATCHES AND UPDATES.....	6
APPLICATIONS, APPLETs, AND PLUG-INS.....	6
MULTI-HOMED COMPUTERS	6
BACKUPS	6
WIRELESS ACCESS.....	6
SEVERABILITY (FACULTY/STAFF/STUDENTS)	6
THEFT	6
USER INDEMNITY	7
COMPLIANCE	7

Houston Community College acquires, develops, maintains and secures all computers, information systems, servers and other electronic communications resources that are connected to HCC's network. These technology resources are reserved for HCC-related purposes, including direct and indirect support of HCC's instruction, research, and service missions; of administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the HCC community and between HCC and the wider local, national, and world communities.

OVERVIEW

The *HCC Guidelines for Security and Acceptable Use* provide specific requirements for the responsibilities of the students, faculty, staff and persons of the general public regarding their use of computer systems, the Internet, and other technology systems provided by Houston Community College System (HCC). Failure to follow these guidelines may result in the loss of data, exposure of sensitive information and compromises of system integrity resulting in security breaches, business interruptions and disciplinary action.

DEFINITIONS

These definitions apply to the terminology used throughout this document.

- HCC User Communities - students, faculty, staff, and persons from the general public
- HCC Community - all HCC campuses, administrative buildings and operating personnel
- Users – students, faculty, staff and persons of the general public
- Technology Resources – Laptops, desktop computers, servers, network equipment, wireless access points, telecom equipment, printers, projectors, cameras, recording devices, peripherals, information systems and facilities such as college IDFs, MDFs, data centers, telecomm rooms, labs and training rooms.
- IT - HCC Information and Instructional Technology departments and staff

APPLICABILITY

These guidelines apply to all HCC users and their use of HCC technology resources on all HCC campuses and remote locations. Additional policies and user guidelines may apply to specific technology resources operated by specific HCC campuses.

GUIDELINES

HCC acquires, develops, maintains and secures technology resources to support the administrative, instructional and community mission of the college. IT staff provide the direct and indirect support for instruction and administrative users and the HCC community and for the free exchange of ideas between HCC users and the local, national, and world communities.

As an institution of higher education, HCC is committed to encouraging and supporting faculty in instructional efforts. Enforcement of the Information Technology policy and these guidelines shall, therefore, ensure preservation of and respect for faculty members' academic freedom. The rights of academic freedom and the freedom of expression apply to the use of college technology resources; however, there are responsibilities and computing limitations associated with these rights. As such, the use of HCC technology resources is subject to the normal requirements of legal and ethical behavior. The user communities must abide by all applicable restrictions and controls, whether or not they are physical, logical or operational controls, or built into the computer operating systems architecture or network infrastructure. Therefore, all members of the user communities must comply with all HCC policies, guidelines, procedures and applicable local, state, and/or federal laws concerning the use of HCC technology resources.

ADMINISTRATIVE RESPONSIBILITY

IT has the direct responsibility to publicize these guidelines to the user communities and to protect their rights while enforcing the guidelines consistent with those rights. HCC also has the authority to control or refuse access to any user who violates these guidelines, threatens the rights of other users, or jeopardizes the operation of any HCC computing equipment or facility.

COMPUTER USAGE

RIGHTS & RESPONSIBILITY

HCC maintains complete ownership of all technology resources. As such, access to HCC's technology resources is a privilege and not a right. Users must respect the rights of other users, respect the integrity of technology resources, and observe all relevant guidelines, laws, regulations, and contractual obligations of HCC.

Permissible use of HCC's technology resources includes but is not limited to:

- Communicating with fellow employees, students, faculty members and professional associations, as necessary to accomplish HCC-related business.
- Acquiring information and resources necessary to perform assigned responsibilities.
- Instructional and administrative purposes.
- Limited personal use, such that it has no adverse effect on an employee's job performance or a student's academic performance.

HCC recognizes that community is essential to the teaching, learning and professional experience. Part of this experience requires communicating with users both inside and outside of HCC. IT supports the use of technology resources for professional as well as personal use as long as personal use:

- Is incidental and not detrimental to other HCC users.
- Imposes no tangible cost on HCC.
- Does not unduly burden the HCC's technology resources.
- Has no adverse effect on an employee's job performance or a student's academic performance.
- Is not for the purpose of personal financial gain.

All HCC users are responsible for protecting the confidentiality, integrity, and availability of HCC data and technology resources.

COPYRIGHT & INTELLECTUAL PROPERTY

Respect for intellectual property, learning, and creativity is essential to academic discourse. This applies to works of authors and publishers in all media and includes respect for the right to acknowledgment and the right to determine the form, manner, and terms of publication and distribution. HCC users must abide by HCC Copyright Infringement and Intellectual Property policies and guidelines pertaining to the copyrighted and intellectual property works of HCC user communities as well as commissioned works of persons from the public Internet domain.

As such, HCC technology resources may not be used for the purpose of downloading or making unauthorized copies of copyrighted materials. While some online materials are public domain, Internet users should generally assume that all online material is copyrighted and not available to be copied or disseminated without permission and proper acknowledgement of the creator. Online material includes all documents, data, websites, software, graphic images, music or streaming media downloaded or otherwise transferred for personal or professional use.

Individual users may be held legally and financially responsible for violations of copyright.

SOFTWARE USE

Software that is developed by, owned by or licensed to HCC is protected by intellectual property and copyright policies and laws as well as software licenses and contractual agreements. Users are not allowed to download or make unauthorized copies of such protected software for personal use or distribution unless explicitly outlined by HCC or in the software contract.

DAMAGE OR IMPAIRMENT OF HCC RESOURCES

The intentional transmission of material that may contain a virus or other harmful or disruptive components is prohibited. This includes the distribution of reckless or negligent e-mail attachments or files that may be damaging to any computer-based system (e.g., by the introduction of any so-called "virus," "worm," "Trojan-horse" and executable file attachment programs).

Damage of HCC resources includes, but is not limited to:

- E-mail systems
- Servers
- Network and telecomm systems
- Database systems and programs
- Electronically stored files
- Instructional and administrative applications, systems and software
- Printing systems
- Data, imaging and file management resources

UNAUTHORIZED COMMERCIAL ACTIVITIES

HCC technology resources are provided by HCC in support of the colleges teaching and learning mission. The use of HCC technology resources for personal or commercial gain or for other personal purposes not officially approved by HCC is prohibited. It is inappropriate to use the technology resources for:

- Commercial gain or placing a third party in a position of commercial advantage
- Commercial advertising or sponsorship not affiliated with HCC
- Any non-college or non-instruction related activity, including online gaming and gambling

COMPUTER HARASSMENT

HCC Harassment and Workplace Violence policies prohibit sexual and discriminatory harassment. HCC technology resources are not to be used to libel, slander, or harass any person. The following constitute, but are not limited to, examples of computer harassment:

- Intentionally using the computer to degrade, harass, terrify, intimidate, threaten or offend another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family.
- Intentionally using the computer to contact another person repeatedly with the intent to degrade, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.
- Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease.
- Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another.
- Intentionally using the computer to invade the privacy (academic or otherwise) of another user, or the threatened invasion of the privacy of another user.

ELECTRONIC MAIL (E-Mail)

E-mail is a primary mode of communication for the college. As such, all HCC users are issued an e-mail account, login, password and storage space which is accessible both on and off site. HCC e-mail systems must not be used to transmit messages which contain, or may be considered to contain, obscene, profane, indecent, violent, threatening, discriminatory or defamatory material or attachments to any person whether or not they are associated with HCC.

RIGHTS & RESPONSIBILITIES

The use of HCC's e-mail system is a privilege, not a right. HCC e-mail users are responsible for the content, dissemination, and management of their e-mail messages and folders. This responsibility means ensuring that e-mail messages sent within or through the HCC e-mail systems:

- Do not contain information that is harmful to HCC or its user communities.
- Are courteous, polite and professional to the intended recipient(s).
- Protect the rights to privacy and confidentiality for all users.

- Do not contain obscene, offensive, or slanderous material or attachments.
- Are not used for purposes that conflict with HCC interests.
- Are for conducting business and instructional purposes unless otherwise authorized and approved by HCC
- Are not used for illegal purposes, or in support of illegal activities;
- Are not used for commercial purposes or political lobbying;
- Are not used for excessive personal use.
- Are not used to interfere with or disrupt the use of e-mail by other users, including but not limited to chain letters, SPAM (unsolicited messages broadcast to large numbers of people), junk mail or illegal schemes or activities.
- Communications that could be considered harassing, including but not limited to racial slurs and obscene language; and
- Anonymous mailing or mailings which impersonate another individual.

CONFIDENTIALITY & SECURITY

Users must understand that e-mail is not a secure medium for transmitting information and should not be considered private or confidential.

The following points are outlined according to how confidentiality and security relate to e-mail:

- HCC e-mail systems and their contents are the property of HCC, which possesses the express right to allow authorized HCC system administrators to monitor and examine the content and security of any electronic information sent through or stored within the HCC e-mail systems.
- All e-mail stored on HCC Servers are subject to Open Records Act/Texas Public Information Act.
- Users must ensure that the format and integrity of their HCC e-mail account password complies with HCC guidelines.
- Sensitive, personal, and confidential content and attachments must not be sent or stored on HCC e-mail systems unless there is a specific professional or business need.
- Users should be aware that messages are not deleted from the e-mail system until all recipients of the message and any forwarded or attached copies have been deleted.
- E-mail messages can be forged in the same way as faxes and memoranda. If a message is suspected of forgery or the origin and identity of the sender is unknown, users should delete the message and not open it.
- Viruses, worms, Trojan Horses, executables, spam, “phishing” and other threats use e-mail to transport and disrupt use. E-mail, attachments or hyperlinks should not be opened unless the user can verify its owner, source, and content.
- HCC users should not reply to e-mail messages requesting confidential information or any requests for logon or personal credentials.

HCC IT staff will not provide personal information or passwords via non-HCC or personal e-mail accounts or over the phone. Users are responsible for contacting HCC Help Desk for instructions and for maintaining and resetting their HCC passwords.

WEB PAGES

HCC websites and pages are designed as a source of vital information for its faculty, students and staff and must present accurate, relevant information about HCC, individual colleges, divisions, or departments. Colleges are responsible for ensuring that their website is effectively managed and provides information that is accurate, pertinent and accessible to all users, including those with disabilities. Unofficial non-HCC related or personal websites and pages shall not include the HCC logo or any reference to Houston Community College that would mislead the user into believing that the information presented is official information or part of HCC’s official website.

Format and content of all official HCC web pages must follow HCC Web Design Guidelines. Users must submit an HCC Web Content Management System Access Request form and attend training before being provided access to the HCC Content Management system and entering online content.

Websites developed and maintained within HCC’s Vignette content management system must comply with the HCC Web Design Guidelines.

SECURITY

HCC employs measures to secure and protect users and their technology resources. HCC provides antivirus software for HCC desktops and laptops. The software must be installed and remain installed on each applicable HCC desktop and laptop with the automatic update capability turned on. Antivirus software information is available from the HCC Help Desk.

Users who are responsible for administering web services, servers or network equipment are also responsible for maintaining all software; firmware and operating system security patch levels. Equipment and services that are not at an appropriate security patch level are a risk to the HCC community and will be disconnected until proper maintenance is completed.

While HCC does not routinely monitor individual usage of its technology resources, the normal operation and maintenance of HCC technology resources requires the backup and caching of data and communications, the logging of bandwidth and Internet activity, the monitoring of general usage patterns and other such activities that are necessary for the rendition of service. Services or activities determined to be disruptive or detrimental to the network will be reported to the Vice Chancellor of Information Technology and reviewed for termination.

Users are responsible for securing their personal computing environments and resources. Users should:

- Become familiar and follow HCC's records retention guidelines.
- Change desktop and network passwords periodically.
- Secure technology resources.

PASSWORDS

Passwords are required when authenticating users with and authorizing access to secure HCC technology resources. Passwords should be kept secret, unshared, unwritten and not stored in an electronic format. All passwords and accounts granting access to HCC network, computing, and storage resources are to be used only by the assigned user of the account and only for authorized purposes.

Passwords are issued and reset by IT. Users are required to change passwords immediately after their initial login and after a password reset. Passwords must have the following characteristics:

- Passwords are to be assigned to individual persons to permit secure access to any network-accessible HCC technology resources.
- Blank or null passwords are not permitted
- Passwords will have a minimum length of seven (7) characters
- Users are not permitted to use their last 3 passwords (password history)
- Users are required to change passwords within a minimum of 120 days
- When possible, passwords should contain upper and lower case letters, numbers and special characters
- Passwords which are obvious, such as nicknames and dates of birth, should not be used.
- Passwords should never be shared with another user.
- Passwords stored on a computer should be encrypted.
- User accounts will be disabled if more than three consecutive invalid passwords are attempted.

Procedures for forgotten passwords will require that the user be personally identified.

VIRTUAL PRIVATE NETWORK (VPN) ACCESS

HCC provides VPN software and access to approved and authorized users. VPN software provides secure and encrypted remote access to HCC's network and services. Users must complete an IT Security Request form and be authorized by their supervisor to have remote access before VPN software and access can be provided.

ACCESS TO SECURE IT AREAS

Access to IT data, telecomm and network facilities is restricted to authorized users. Users must have approval from the Vice Chancellor of Information Technology or designee before accessing restricted IT areas at all colleges.

PATCHES AND UPDATES

HCC computers are configured to automatically download operating system security and antivirus software patches and updates in order to protect users. The automatic download feature should not be circumvented, uninstalled or turned off. All operating system and antivirus patch levels must be maintained by the responsible user or administrator in order to access the HCC network.

MULTI-HOMED COMPUTERS

Multi-homed computers have two or more network adapters that each access different networks. Multi-homed computers or servers that access both public and private networks are prohibited.

BACKUPS

HCC does not offer file recovery services for user laptops and desktop computers. Data is vulnerable to human or system error and theft. Users are responsible for the backup and security of their data and files. Critical data files that are saved on a laptop or desktop computer should be routinely copied to or backed up to the user's network-addressable drive provided by IT or to removable media and stored in a secure place. Data stored on the network-addressable drives will be backed up daily and stored offsite.

WIRELESS ACCESS

Using a wireless network involves broadcasting network traffic via radio frequency bands. Secure connections, authentication, and encrypting traffic are used to ensure data security while using wireless technology. HCC wireless networks will require secure client connections and authentication before HCC data transmission is permitted.

The deployment and use of HCC-owned wireless devices, unlicensed wireless devices and other unauthorized wireless devices connected to the HCC network infrastructure are subject to but not limited to the following restrictions:

- All use of wireless access points and devices must comply with applicable laws, regulations (FCC), and HCC guidelines.
- HCC IT personnel are responsible and accountable for the operation of the HCC wireless network and access points.
- Usage of HCC's wireless network will be automatically logged and maintained for an extended period of time.
- Wireless access points connected to the HCC network without prior authorization of IT are prohibited and will be disconnected from the HCC network.

SEVERABILITY (FACULTY/STAFF/STUDENTS)

HCC terminates the access of fulltime employees and students to e-mail accounts when users terminate or leave the institution unless other arrangements are made. Part-time faculty are allowed to maintain their e-mail accounts for one-year after the end date of their last assignment in order to maintain contact with their students and department chairs.

HCC faculty and staff agree to:

- Return any and all HCC computers, software and peripheral devices upon termination of employment.
- Forfeit, remove and/or delete any data, files, applications or programs on personally-owned computers used in the commission of business-related services for HCC.

HCC reserves the right to withhold replacement costs for any and all non-returned computers or other equipment, and for the intentional or unintentional misuse or destruction of computer equipment or property (beyond normal wear and tear) of HCC.

THEFT

Users must report the loss or theft of technology resources to the College Police within 48 hours of knowledge of the loss. Users will be held accountable for reimbursing HCC at the depreciable value or 40% of value of the technology resources whichever is greater for lost or stolen technology resources issued by HCC.

USER INDEMNITY

HCC shall not be liable for users' inappropriate use of technology resources, violations of copyright restrictions or other laws, user mistakes or negligence, or costs incurred by users.

Users of the technology resources agree to indemnify and keep indemnified HCC, all executives, and every member of its Board, faculty and staff against all actions, claims, and demands resulting from:

- Infringement of patent and or breach of copyright which may be brought or made against HCC or any member of its staff arising out of, or in connection with, the use of HCC computing facilities.
- The non-delivery or loss of any e-mail messages, content, data or attachments due to improper use or any other unforeseen circumstance.

COMPLIANCE

HCC users must act in a professional and respectful manner at all times. Users are obligated to understand and follow all HCC policies and guidelines and to obey the laws, rules, policies, contracts, licenses, laws of libel, privacy, copyright and trademark as described by the *Electronic Communications Privacy Act*, the *Computer Fraud and Abuse Act*, *US Copyright Laws* and the *Computer Crimes Section of the Texas Penal Code (7 Section Penal Code, section 33)*.

As such, users are prohibited from intentionally:

- Maintaining, creating or transmitting through electronic means, any harassing images or offensive messages to be construed by others to be of degrading, threatening, libelous, sexual, racial, or religious-nature in any content or form.
- Attempting to monitor read, copy, change, or delete another users or entities files or software from an HCC technology resource.
- Running, installing, or distributing to another computer system, any program, worm or virus which could result in damage to files or the computer system, by immediate action or reproduce itself for dormant or latent malicious actions.
- Attempting to circumvent data protection schemes or exploit security loopholes at any HCC facility.
- Using a computer without the consent of its owner or accessing data stored in a computer system without the consent of its owner.
- Providing passwords or similar confidential information about a computer security system to another person without the consent of the person employing the security system for the purpose of restricting access to a computer or its data.
- Causing a computer to malfunction or to interrupt operation of a computer system without the consent.
- Altering, damaging, destroying data, or destroying a computer program in a computer without the consent of the owner or licensee of the data or computer program.
- Transmitting HCC business-sensitive confidential information to non-HCC personnel.
- Gaining unauthorized electronic access to HCC technology resources or those of any other institution, organization, or individual person through the use of false or misleading information for the purpose of obtaining access to unauthorized resources.
- Performing acts which are wasteful of computing or networking resources or which unfairly monopolize resources to the exclusion of others—including, but are not limited to, sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, online gaming or gambling or obtaining unnecessary output or printed material.
- Using a computer or network ID or password that is assigned to another student, faculty, or staff, unless permission has been authorized by that person for use in troubleshooting and maintaining the integrity of the computer system or network.
- Attempting to obtain or change a password on another computer or network environment unless explicitly granted permission to do so by the owner of the system for purposes of gaining access to a computer or network environment that has the owner locked out of the system.
- Causing the theft or mutilation of any HCC computer property, or cause the unacknowledged or unauthorized appropriation of another person's computer program or applications, or exploit any data of any computer system, in whole or in part, for a computer-related exercise.

- Accessing, altering, copying, moving or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system without prior authorization.
- Bypassing any software licensing agreements and copyright laws when installing for general, business, or personal use on a HCC computer used in the commission of HCC business.
- Making copies of copyrighted software, unless that software vendor has issued a license which specifically allows for the copying of that software to be used for backup or archiving purposes.
- Accessing network closets, data centers, telecomm rooms or other secured areas without authorization.
- All other intentional activities that would violate the laws, rules and HCC Board Policies.

Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses internal and external to the HCC computing environment.

HCC reserves the right to:

- Limit or restrict any user's usage of technology resources for violations of these guidelines.
- Copy, remove, or otherwise alter any information or system that may undermine the use of the technology resource; and can do so with or without notice to the user in order to protect the integrity of the HCC computing environment against unauthorized or improper usage, and to protect authorized users from the effects of unauthorized or improper usage.
- Institute emergency action to safeguard the confidentiality, integrity and availability of the technology resources up to and including the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords.
- Terminate access to computing systems and associated networks for infringement of patents, breach of contracts or use for commercial or non-HCC related activities.
- Periodically run unannounced software audits of any and all technology resources owned by HCC.
- Track and monitor user accounts, activity and resource usage, without notice, when requested by the Chancellor, Deputy Chancellor or General Counsel.
- Disclose the results of any general or individual monitoring, including the contents and records of individual communications, to appropriate HCC personnel and law enforcement agencies.

If any person at HCC becomes aware of the misuse of a technology resource or is offended, humiliated, intimidated or embarrassed by the use of e-mail or the Internet by others, the person should immediately report it to the following:

- Student: College Dean of Students, Campus Police or Vice Chancellor of Student Services
- Faculty: Department Chair, Vice Chancellor of Instruction or General Counsel
- Staff: Supervisor, President, Vice Chancellor of Information Technology or General Counsel

Violations of HCC policies and guidelines may result in the following disciplinary action or actions:

- Counseling
- Suspension or restriction of access to technology resources
- Suspension or expulsion from HCC
- Termination of employment
- Criminal prosecution under applicable local, state and federal statutes
- Personal liability
- Other disciplinary action consistent with HCC policies and procedures, including but not limited to the Student Handbook

The Chancellor or designee may appoint a committee to investigate and address violation of this policy or related procedures, guidelines, or user agreements.