

# *Holmes Community College*

## *Information Technology Use Policy*

### *General*

Holmes Community College is dedicated to providing the best possible services to its employees and students and is committed to ensuring that the information system resources are used appropriately for the purposes they are intended. This policy governs the use of all computers, computer-based communications, networks, and all related equipment (including career/technical equipment) administered by Holmes Community College, referred to hereafter as HCC. This policy is designed to help you understand the expectations for the use of the resources provided. Restrictions placed on use are to protect the resources and integrity of the network and to comply with all local, state, and federal laws and regulations. By using these facilities and equipment the user acknowledges consent to abide by this policy.

### *Authorized Users*

An authorized user is defined as any employee, student, or guest that has completed the Information Technology Use Agreement Form and/or has been approved by the Information Technology Department, referred to hereafter as IT.

For students, the agreement form will be part of the enrollment application.

### *Appropriate and Acceptable Use*

The computer facilities, equipment, and software of HCC are to be used only by authorized users. Appropriate use is defined as official business conducted by authorized users. However, occasional or incidental use by authorized users for personal, non-business purposes is acceptable, as is the case with personal phone calls, provided that all use is compliant with this policy. Users need to demonstrate a sense of responsibility and may not abuse the privilege. The user should be aware that any communications, files or use of HCC information systems resources are not to be considered private or confidential, regardless of passwords and deletions, and may be monitored, searched and/or archived at any time. HCC reserves the right to prohibit access to certain sites, material and programs. If questions arise as to whether a specific activity complies with appropriate and acceptable use, contact IT.

---

The following are some guidelines for appropriate and acceptable use:

- Be polite. Do not be abusive in your communications or emails to others.
- Use appropriate language. Do not use obscene language, vulgarities, sexually suggestive or any language that may be derogatory toward race, religion, ethnicity, or gender.
- Communications should be in a professional manner and not reflect negatively upon HCC.
- Proper email etiquette is recommended.
- Email groups have been created to easily communicate business related information to faculty and staff. Refrain from using these addresses for non-business related material.
- Alternate means of delivery should be considered when sending large attachments especially to multiple recipients.
- Users are responsible for the physical condition of the equipment that they are operating. User shall not break, disassemble or otherwise cause damage to any computer or computer related equipment.
- Sharing of resources or access to resources between students, faculty and staff must be approved by IT.
- If you learn of a virus alert or security threat, report it only to IT for evaluation immediately. Do NOT take any other action.

The following are expressly prohibited:

- Violating any local, state or federal laws and regulations while using HCC facilities and equipment.
- Viewing, storing or distributing obscene, pornographic or objectionable material.
- Participating in gambling.
- Downloading or distributing or attempting to download or distribute pirated software or data.
- Deliberately propagating any virus, worm, Trojan horse, or trap-door program code.
- Disabling or overloading or attempting to disable or overload any system or network.
- Attempting to hide your identity or represent yourself as someone else when sending email or any other type of communication.

- Intentionally causing network congestion <sup>1</sup> or significantly hampering the ability of other users to access resources.
- Disclosing any confidential or HCC information unless granted by HCC.
- Violating copyright laws to include copy, retrieve, modify, or forward copyright materials except as permitted by the copyright owner.
- Using HCC information systems resources for soliciting, personal financial gain, partisan political activities or distributing “junk” email such as chain letters or spam.
- Engaging in any activity that may disrupt the use of resources for other users.
- Using the messenger service. This service is to be utilized only by IT.
- Installing servers, workstations, or notebook computers onto the network for any intention. Installations must be approved by IT prior to installation to insure the security and integrity of the network.

## **Software**

Software programs, including but not limited to, Internet downloaded programs, utilities, add-ins, shareware, freeware, Internet access software, patches, or upgrades, shall not be installed, removed or altered on any desktop, laptop, or server without prior approval from IT. The software on each computer will be inventoried on a regular basis to ensure compliance. Software owned or licensed by HCC may not be copied to alternate media except for backup purposes, distributed by email, transmitted electronically, or used in its original form on other than the equipment it was licensed for. In no case is the license agreement or copyright to be violated. Software licensed to HCC is to be used for its intended purpose according to the license agreement. Users are responsible for using software in a manner consistent with the licensing agreements of the manufacturer.

## **Hardware**

Modifications or additions are not allowed without prior approval from IT. Do not relocate hardware unless it is approved by the person responsible for the equipment and a transfer form has been completed and delivered to Inventory Personnel. Information systems equipment should not be removed from the premises of HCC without the permission from the department head and/or Inventory Personnel. In the event equipment is to be off premises for an extended time, the employee responsible for the equipment must file a written hand receipt with Inventory Personnel. Mobile equipment such as notebook computers, projectors, and cameras used in daily offsite work may be taken off campus by the person it was assigned to.

## **Security**

Important and sensitive data is processed and stored on HCC computer systems. Local area networks (LAN), wide area networks (WAN), and the Internet increase the risk that data can be inappropriately accessed and used. Usernames and passwords are for the use of the specifically assigned user and are to be protected from abuse and/or use by other individuals. HCC has implemented several security measures to assure the safety and integrity of the network and data. Anyone who attempts to disable, defeat or circumvent any security measure will be subject disciplinary action.

- Do NOT give your password to anyone other than IT.
- Do NOT post your password in a readily accessible area (ex. On monitor, an unlocked desk drawer).
- Do NOT leave your computer logged on while not in use.
- Do NOT use someone else’s account
- Do NOT let someone use a computer while logged on with your account.
- Do NOT allow someone to connect a computer to the HCC network without approval from IT.
- Do NOT attempt to hack/crack<sup>2</sup> passwords
- Do NOT attempt to hack/crack into any systems.
- Do NOT engage in any activity<sup>3</sup> which may compromise the security of HCC electronic data, computer systems, internal networks, or external networks.

---

<sup>1</sup> Network Congestion – An excessive amount of traffic on the network, to the point where messages or other electronic communications are slow or blocked causing network performance to be adversely affected.

<sup>2</sup> Hack/Crack – To gain entry to a system to explore, destroy, alter and/or move data or resources in such a way that could cause injury or expense to others, or lead to the gathering of sensitive information.

<sup>3</sup> Security compromising activity – To freely give to unauthorized personnel ones user ID/passwords, HCC dial-up access numbers, internal IP numbers, and/or computer or server names or install unauthorized software are a few examples.

- Do NOT use any wireless devices without authorization from IT. This includes, but is not limited to, routers, hubs, or modems.
- Do NOT connect computer systems to the network while modems are in use.
- Do NOT create additional domains or workgroups.
- Do NOT connect any hardware to the HCC network without prior approval from IT.

### **Data Backups**

Even though IT maintains regular backups, it is the sole responsibility of each user to backup data that is important to them. Space has been reserved on selected servers for each employee to store important business related material. Do not store non-business related material in this space. Some classes provide network storage for students. This space is reserved for classroom material only. IT performs a daily backup of all network data files and system files. A complete backup is stored offsite monthly in the event of theft, fire, or other major disaster. This backup does not include data on each workstation.

### **Reliability**

HCC/IT makes no warranties of any kind, whether expressed or implied, for the services that it is providing. HCC/IT will not be responsible for any damages you suffer, including, but not limited to, loss of data, delays, non-deliveries, incorrect deliveries, or service interruptions.

### **Violations**

All users are required to report any violations of this policy immediately to IT.

The Copyright Act of 1976 (amended in 1984) imposes fines up to \$250,000 and up to two years imprisonment for first offenders who have willfully infringed a software copyright. The aim is to deter and punish software criminals. The law also applies to individuals and businesses that misuse copyrighted software. All copyright violations at HCC should be reported to IT so appropriate action can be taken to ensure HCC is operating within the scope of the law.

Any user who violates this policy is subject to disciplinary action which may include paying for damages, fines, denial of access to technology resources or other remedies applicable under local, state or federal laws or regulations. Faculty and Staff may also be subject to probation, suspension, or termination. Students may also be subject to suspension, expulsion, and /or other remedies as outlined in school and district policies. Furthermore, in the event of any illegal activity, the user may also be reported to the appropriate law enforcement authority which may result in criminal or civil prosecution. HCC will fully cooperate with law enforcement during an investigation.

### **Revisions**

This policy is subject to revision at any time. It is the user's responsibility to conform to the current policy.

---

# *Holmes Community College*

## *Information Technology Use Policy Agreement Form*

I have read and understand the Holmes Community College Information Technology Use Policy. I agree to abide by the terms and conditions as stated. I further understand that any violation of the policy is unethical and may constitute a violation of law. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken. I may be subject to probation, suspension or termination.

\_\_\_\_\_  
Employee's Full Name (please print)

\_\_\_\_\_  
Employee's Signature

\_\_\_\_\_  
Date

# *Holmes Community College*

## *Information Technology Contacts*

Kevin Baker	Director of Information Technology	<a href="mailto:kbaker@holmescc.edu">kbaker@holmescc.edu</a>
Justin Ferguson	Network Administrator	<a href="mailto:jferguson@holmescc.edu">jferguson@holmescc.edu</a>
Jesse Nichols	IT Specialist	<a href="mailto:jnichols@holmescc.edu">jnichols@holmescc.edu</a>
Mitch Costilow	IT Specialist	<a href="mailto:mcostilow@holmescc.edu">mcostilow@holmescc.edu</a>
Josh Neagle	IT Specialist	<a href="mailto:jneagle@holmescc.edu">jneagle@holmescc.edu</a>
Patsy Vaughn	Programmer/Analyst	<a href="mailto:pvaughn@holmescc.edu">pvaughn@holmescc.edu</a>
Tammy Smith	Programmer/Analyst	<a href="mailto:tsmith@holmescc.edu">tsmith@holmescc.edu</a>
Jimmy Hall	Programmer/Analyst	<a href="mailto:jihall@holmescc.edu">jihall@holmescc.edu</a>
Kelly Blaylock	Report Analyst	<a href="mailto:kblaylock@holmescc.edu">kblaylock@holmescc.edu</a>
Wesley Lepard	Help Desk	<a href="mailto:wlepard@holmescc.edu">wlepard@holmescc.edu</a>