WILLIAM CAREY UNIVERSITY

INFORMATION TECHNOLOGY DEPARTMENT

Acceptable Use Policy

Version 1.0 – January 5, 2011

498 Tuscan Avenue, Box 147

Hattiesburg, MS 39401

Phone 601.318.6203 • Fax 601.318.6546

Introduction

As part of its educational mission, the William Carey University acquires, develops, and maintains computers, computer systems and networks. These computing resources are intended for university-related purposes, including direct and indirect support of the university's instruction, research and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas within the university community and among the university community and the wider local, national, and world communities.

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may govern specific computers, computer systems or networks provided or operated by specific units of the university. Consult the operators or managers of the specific computer, computer system, or network that you are interested in for further information. This policy may be modified as deemed appropriate by the University. Users are encouraged to periodically review the policy as posted on the university's home page.

Rights & Responsibilities

The rights of academic freedom and freedom of expression apply to the use of university computing resources. So too, however, do the responsibilities and limitations associated with those rights. The university supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. However, the use of university computing resources, like the use of other university-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible.

General Rules

Users of university computing resources must comply with federal and state laws, university rules and policies, and the terms of applicable contracts including software licenses while using university computing resources. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities; the university's Student Code of Conduct; the university's Sexual Misconduct Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions as to how the various laws, rules and resolutions may apply to a particular use of university computing resources should contact the Information Technology Department for more information.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using university computing resources. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate account administrator, Coordinator of Network and Infrastructure Services, and/or Dean, Director, or Department Chair.

Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of university computing resources, the university may require users of those resources to limit or refrain from specific uses if, in the opinion of the Coordinator of Network and Infrastructure Services, such use interferes with the efficient operations of the system.

Users may not state or imply that they speak on behalf of the university or use university trademarks and logos without authorization to do so. Authorization to use university trademarks and logos on university computing resources may be granted only by the Information Technology Department. The use of appropriate disclaimers is

encouraged. For further guidelines on the use of the university's marks, name and image, please contact the Information Technology Department.

Users must not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of WCU computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing malware applications. Deliberate attempts to circumvent data protection or other security measures are not allowed.

Enforcement

Users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the university disciplinary procedures applicable to the user. The university may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Security & Privacy

The university employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that the university cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users should also be aware that their uses of university computing resources are not completely private. While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The university may also specifically monitor the activity and accounts of individual users of university computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to a Web page;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability;
- There is reasonable cause to believe that the user has violated or is violating this policy;
- An account appears to be engaged in unusual or unusually excessive activity; or it is otherwise required or permitted by law.

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate Coordinator of Network and Infrastructure Services or the Director of Information Technology. The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

Users are responsible for all activity associated with their accounts and devices. Any and all activity associated with a user's account or device will be considered action by the account or device owner. Therefore, using another user's credentials is strictly prohibited and is grounds for removal from all WCU networks.

Visitors to WCU Web sites who are not currently WCU students, faculty or staff should refer to the university's Online Privacy Policy for privacy information.

E-Mail

For purposes of this document, e-mail includes point-to-point messages, postings to newsgroups and listserves and any electronic messaging involving computers and computer networks. Organizational e-mail accounts, including those used by student organizations, are held to the same standards as those for individual use by members of the William Carey University community.

SaderApps email is the official email account for students.

Examples of Inappropriate Uses of E-mail: While not an exhaustive list, the following uses of e-mail by individuals or organizations are considered inappropriate and unacceptable at William Carey University. In general, e-mail shall not be used for the initiation or re-transmission of:

- Chain mail that misuses or disrupts resources - E-mail sent repeatedly from user to user, with requests to send to others;
- Harassing or hate-mail - Any threatening or abusive e-mail sent to individuals or organizations that violates university rules and regulations or the Code of Student Conduct;
- Virus hoaxes;
- Spamming or e-mail bombing attacks - Intentional e-mail transmissions that disrupt normal e-mail service;
- Junk mail - Unsolicited e-mail that is not related to university business and is sent without a reasonable expectation that the recipient would welcome receiving it; and
- False identification - Any actions that defraud another or misrepresent or fail to accurately identify the sender.

Commercial Use

Computing resources are not to be used for personal commercial purposes or for personal financial or other gain. Occasional personal use of university computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of University equipment.

Network Infrastructure/Routing

Users must not attempt to implement their own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to WCU IT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS.