Heritage Christian University

Student Information Technology Acceptable Use Policy

1.0 Overview:

The IT Department is committed to protecting Heritage Christian University's employees, students, partners and the university from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, and electronic mail are the property of Heritage Christian University. These systems are to be used for educational purposes in serving the interests of the university, and of our students in the course of normal operations.

Effective security is a team effort involving the participation and support of every HCU student who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at Heritage Christian University.

These rules are in place to protect the student and HCU. Inappropriate use exposes HCU to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope:

This policy applies to all students using the HCU provided network or equipment.

4.0 Policy:

4.1 General Use and Ownership

4.1a Students are responsible for exercising good judgment regarding the reasonableness of personal use.

4.1b For security and network maintenance purposes, the IT Department may monitor equipment, systems and network traffic at any time.

4.1c The IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a student of HCU authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing HCU-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities
The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by HCU or the student.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or movies, and the installation of any copyrighted software for which HCU or the end user does not have an active license.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others.

6. Using an HCU computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any HCU account.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorized to access.. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

9 Port scanning or security scanning.

10. Executing any form of network monitoring which will intercept data not intended for the student's host.

11. Circumventing user authentication or security of any host, network or account.

12. Interfering with or denying service to any user other than the student's host (for example, denial of service attack).

13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

14. Providing information about, or lists of, HCU students or employees to parties outside HCU.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Blogging

1. Blogging by students, whether using HCU's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Use of HCUs systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate HCU's policy, and is not detrimental to HCU's best interests. Blogging from HCU's systems is also subject to monitoring.

2. Students are prohibited from revealing any HCU confidential or proprietary information, trade secrets or any other material covered by FERPA guidelines.

3. Students are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by HCU.

4. Students may not attribute personal statements, opinions or beliefs to HCU when engaged in blogging. Students assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, HCU's trademarks, logos and any other HCU intellectual property may not be used in connection with any blogging activity without permission.

Social Networks

1. The use of social networks such as Facebook, Google+, and MySpace is also subject to the terms and restrictions set forth in this Policy. Any form of harassment or illegal use of social networks is strictly prohibited.

5.0 Enforcement

Any student found to have violated this policy may be subject to disciplinary action, up to and including expulsion.