



ACCEPTABLE COMPUTING USE POLICY FOR GUESTS

SUBJECT: Acceptable Computing Use Policy for Guests of University Resources
RESPONSIBLE UNIT: Information Technology Services (ITS)
REFER QUESTIONS TO: Information Security Officer
ISSUE DATE: August 29, 2008

APPROVED BY:

A handwritten signature in black ink, appearing to read "Mo Qayoumi".

Mo Qayoumi, President, CSU East Bay

DISTRIBUTED TO: CSUEB Guests & Campus Community

"To provide an academically rich, multicultural learning experience that prepares all its students to realize their goals, pursue meaningful lifework, and to be socially responsible contributors to their communities, locally and globally." – University Mission Statement

"The University values learning in an academic environment that is inclusive and student-centered. We value engagement in the civic, cultural and economic life of the communities we serve -- locally, regionally, and globally. We value critical and creative thinking, effective communication, ethical decision-making, and multi-cultural competence. We value the open exchange of ideas and viewpoints." – University Values Statement

1.0 PURPOSE

California State University, East Bay (CSUEB) is a public institution fully committed to the ideals of intellectual and academic freedom, freedom of expression and multicultural diversity. CSUEB provides access to technology resources (e.g., computing hardware, software, electronic information systems, networks, etc.) for purposes related to its mission and to the responsibilities and necessary activities of its faculty, students and staff. These resources are vital for the fulfillment of the academic, research and business needs of the CSUEB community. To promote and protect these ideals and resources, this policy is intended to define acceptable and unacceptable computing uses and practices for guests on the university campuses.

CSUEB has created this Acceptable Use Policy (the "Policy") so you will understand when and under what circumstances we may suspend or terminate your use of computing service (the "Service") and access to CSUEB sites containing information and data available via your computer and/or a wireless device (the "CSUEB Sites"). By using our computing Service or accessing CSUEB Sites, you consent to the acceptable use practices described in this Policy, that we may modify from time to time.

Our goal is for all of our subscribers to have an easy and productive experience every time they access the CSUEB Sites or use our Service. Therefore, you may only use our Service for lawful purposes and in a manner that does not interfere with use by other subscribers or our systems. To assure this, we reserve the right, but are not obligated, to suspend or terminate your access to the CSUEB Sites and/or your use of the Service at any time, if we determine in our sole discretion that your conduct on the CSUEB Sites or our Service involves such behavior.

2.0 DEFINITION

Guests are any non-employee and non-student visitors accessing CSUEB computing Service or resources.

3.0 SCOPE

This policy exists within the framework of existing CSUEB policies and applicable state and federal laws that may be related to the use of technology resources. CSUEB provides access to computing resources with the following notification:

- **Information on the Network.** The availability of networked information via CSUEB's computing Service or resources does not constitute endorsement of the content of that information by CSUEB.
- **Illegal Use.** The University does not encourage or condone unethical or illegal use of computing resources. Violation of applicable laws or university policy may result in suspension of computing privileges and/or in appropriate disciplinary or criminal action. The University will not provide legal defense for illegal use of its computers or software.

4.0 GUEST RESPONSIBILITY

You are solely liable for any transmissions you initiate through our computing Service or any content you disclose. Unless you are participating in an area of CSUEB or Service that requires or allows anonymity, you will always use your real name in online communications. You agree to indemnify and hold us harmless from any claim, action, demand, loss, or damage (including attorneys' fees) made or incurred by any third party arising out of or relating to your violation of this Policy.

5.0 POLICY

5.1 Requirements for Good Judgment and Reasonable Care

You are expected to use good judgment and reasonable care in order to protect and preserve the integrity of the equipment, its data and software, and its access.

Examples of inappropriate use are as follows:

- **Harmful or Offensive Content:** Uploading, downloading, posting, distributing, publishing, or otherwise transmitting (collectively,

- "Disclosing") any message, data, information, image, text, or other material (collectively, "Content") that is unlawful, libelous, defamatory, slanderous, obscene, pornographic, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory, or otherwise harmful or offensive;
- **Dangerous Content:** Disclosing any Content that would constitute or encourage a criminal offense, violate the rights of any party, or that would otherwise create liability or violate any local, state, national, or international law;
 - **Infringing Content:** Disclosing any Content that may infringe any patent, trademark, trade secret, copyright or other intellectual or proprietary right of any party. Infringement may result from the unauthorized copying and posting or distributing ring tones, graphics, pictures, photographs, logos, software, articles, music, or videos. By posting any Content, you represent and warrant that you have the lawful right to distribute and reproduce such Content;
 - **False Representation:** Impersonating any person or entity or otherwise misrepresenting your affiliation with a person or entity without proper consent to do so;
 - **Interference:** Interfering with other users of Services;
 - **Deceptive Content or Spam:** Using e-mail, text messaging services , or multimedia messaging services to Disclose deceptive Content-such as letters relating to pyramid schemes, or communications offering or disseminating fraudulent goods, services, schemes, or promotions-or any form of unsolicited commercial e-mail or "spam" (electronic messages sent to multiple e-mail addresses or wireless devices where the recipient has not consented to receive such messages, except messages whose primary purpose is to facilitate, complete, confirm, provide, or request information about a commercial transaction, an existing employment relationship, or an existing commercial relationship that the recipient has previously agreed to enter into with the sender).
 - **Unapproved Promotions or Advertising of Goods or Services:** Without our prior written permission, Disclosing any unsolicited promotions of goods or services, commercial solicitation or any advertising, promotional materials, or any other solicitation of other users for goods or services except in those areas (e.g., a classified bulletin board) that are designated for such purpose;
 - **Off-Topic Content:** Disclosing any Content that is off-topic according to the description of a group or list or sending unsolicited mass e-mailings if such Content is not appropriate to the context and/or purpose of the discussion, group or list;

- **Content Harmful to Other Systems:** Disclosing harmful Content, including without limitation, viruses, Trojan horses, worms, time bombs, zombies, cancelbots, or any other computer programming routines that may damage, interfere with, surreptitiously intercept or expropriate any system, program, data, or personal information.

5.2 Network Usage

Violations of system or network security are prohibited, and may result in criminal and civil liability. CSUEB may investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- **Modifications to Transmissions:** Installation of any amplifiers, enhancers, repeaters, or other devices that modify, disrupt, or interfere in any way with the radio frequency licensed to us to provide Service.
- **Hacking:** Unauthorized access to or use of data, systems, or networks, including any attempt to probe, scan, or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
- **Interception:** Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- **Intentional Interference:** Interference with service to any user, host, or network including, without limitation, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, or broadcast attacks.
- **Falsification of Origin:** Forging any TCP-IP packet header, e-mail header, or any part of a message header.
- **Avoiding System Restrictions:** Using manual or electronic means to avoid any use limitations placed on the Services.

6.0 PROHIBITION AGAINST UNAUTHORIZED BROWSING, USE OR RELEASE OF PRIVATE INFORMATION

The University supports and protects the concepts of privacy and protects the confidentiality of personal information maintained in educational, medical or employment records. Unauthorized browsing, alteration or access of university files and computing devices is strictly prohibited.

7.0 ACCESSING INFORMATION IN PUBLIC AREAS

Public areas (e.g., library facilities, meeting rooms, lawns, etc.), are designed to facilitate the implementation of the University's mission. These learning and meeting spaces combine cyber and physical facilities to foster individual and collaborative teaching and learning, and encourage communication and the exchange of ideas. To that end, the University promotes intellectual and academic freedom. Nevertheless, accessing information resources within public areas comes with the responsibility to be considerate of others when downloading, viewing, storing, or transmitting materials. The University will balance your rights to access the information you choose with the needs of others to work and study in a setting free of intimidation, harassment, or hostility.

8.0 ENFORCEMENT OF THIS POLICY

The University reserves the right to strictly enforce this Policy by, without limitation, issuing warnings, suspending, or terminating Service, refusing to transmit, removing, screening, or editing Content prior to delivery or actively investigating violations and prosecuting them in any court or appropriate venue. We may block access to certain categories of numbers (e.g. 976, 900, and certain international destinations) or certain sites at any time in our sole discretion. We may access, use, and disclose transaction information about your use of our Service, and any Content transmitted by you via CSUEB Sites or through the Service, to the extent permitted by law, in order to comply with the law (e.g., a lawful subpoena); to enforce or apply our subscriber agreements; to initiate, render, bill, and collect for our Services; to protect our rights or property, or to protect users of our Services from fraudulent, abusive, or unlawful use of, or subscription to, our Service.

9.0 REVISION HISTORY

This policy is based on the California State University Chancellor's Office Acceptable Use Policy for Guests (effective: June 1, 2006) and will be subject to revision in response to changes in technology or CSUEB operational initiatives.

Review/Revision Date	Committee/Approving Official
Issue date of initial draft: October 12, 2007	University Information Technology (UIT) Advisory Committee
Legal Review: October 13, 2007	University Counsel (Eunice Chan)
Administrative Reviews: November 1, 2007	Cabinet & Provost Council
Shared Governance Review: Nov 6, 2007	Academic Senate ExCom
Review of Final Draft: Nov 8, 2007	UIT
Approved: November 12, 2007	CIO (John Charles)
Updated for President's signature: August 26, 2008	President (Mo Qayoumi)