

Baker College

Student Computer Acceptable Use Policy

1.0 Overview

Baker College has adopted this Acceptable Use Policy to protect the College and its employees, students, and partners from any inappropriate, 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, computer files, storage media, network accounts, electronic mail, instant messaging, web browsing, and file transfers or downloads are the property of Baker College.

2.0 Purpose

The purpose of this policy is to outline the appropriate and acceptable use of computer equipment and data at Baker College.

3.0 Scope

This policy applies to all students at Baker College when using the College's computing or telephone networks or services.

4.0 Policy

4.1 General Use and Ownership

1. Student computer accounts are created at Baker College for all registered students; accounts are deleted when the student has not registered for class for two or more consecutive quarters.
2. While Baker College desires to provide a reasonable level of privacy, users should be aware that the data created or stored on any computer workstation or server remains the property of Baker College. Because of the need to protect the security of the Baker College network and computer system, the College cannot guarantee the confidentiality of information stored on any network device belonging to the College.
3. Computing resources shall be used in a manner consistent with the instructional and administrative objectives of the College. You are expected to use computing resources in a responsible and efficient manner.
4. For security and network maintenance purposes, authorized individuals within Baker College may monitor equipment, systems and network traffic at any time to ensure compliance with this policy.

4.2 Authorized Use

You use services provided by Baker College whenever you use a college-owned computer, phone or data circuit, software, or network resource. When you use Baker College services you agree to the following conditions:

1. To respect the privacy of other users; for example, you shall not intentionally seek information on, obtain copies of, or modify files or passwords belonging to other users of the College, or represent others, unless explicitly authorized to do so by those users.
2. To respect the legal protection provided by copyright and licensing of programs or data; for example, you shall not make copies of a licensed computer program to avoid fees or to share with other users.
3. To respect the intended usage of an account; for example, you shall not use your college-provided email account or network access to operate a business.
4. To respect the integrity of the network; for example, you shall not intentionally develop or use programs, transactions, data, or processes to harass other users or infiltrate the system or damage or alter the software or data components of a system.
5. To respect the financial structure of a telephone, computing, or networking system; for example, you shall not develop or use any unauthorized mechanisms to alter or avoid charges levied by the College or any of its providers.
6. To respect the rights of other users; for example, you shall comply with all College policies regarding sexual, racial, and other forms of harassment, and you shall not divulge sensitive personal data concerning faculty, staff, or students to which you have access.
7. To adhere to all other Published Policies and Procedures at Baker College.

Other departments of Baker College may have additional terms or conditions of use that apply to specific services offered by the College, such as in Residence Halls, Libraries or Learning Centers

4.3 Unacceptable Use

The following activities are, in general, prohibited.

Under no circumstances is a student of Baker College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing any Baker College-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 system and network activities are strictly prohibited:

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 Baker College.
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, and the installation of any copyrighted software for which Baker College or the end user does not have an active license is strictly prohibited.

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Using a Baker College 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.
5. Making fraudulent offers of products, items, or services originating from any Baker College account.
6. Effecting security breaches or disruptions of network communication. Port scanning or security scanning is expressly prohibited unless prior approval is received from the Computer Information Systems department.
7. Executing any form of network monitoring which will intercept data not intended for the student.
8. Circumventing user authentication or security of any host, network or account.
9. Interfering with or denying service to any user, except as authorized by the Computer Information Systems department.

Email and Communications Activities

The following email and communication activities are strictly prohibited:

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".
6. Use of unsolicited email originating from within Baker College's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Baker College or connected via Baker College's network.

4.4 Peer-to-Peer File Sharing at Baker College

Baker College is committed to reducing the illegal uploading and downloading of copyrighted works through peer-to-peer (P2P) file sharing on campus or residence hall networks. Students and employees need to be aware that such illegal distribution of copyrighted materials may subject them to criminal and civil penalties.

1. Baker College prohibits the use of all P2P applications such as BitTorrent and Limewire. In compliance with this policy these technologies are blocked and anyone attempting to circumvent the block is in violation of this policy. Users in violation of College policy are subject to disciplinary action in accordance with their position at the College.
2. If you are using Baker College's computer network, including any classrooms or laboratories, offices, residence halls, or College-provided wireless connections, the College is your Internet Service Provider (ISP). The Digital Millennium Copyright Act of 2008 requires Baker College to block access to copyrighted materials in a timely fashion when notified that users on its network are sharing copyrighted files.

3. Complaints typically arrive directly from software, music, and motion picture associations, law firms, and copyright holders in the form of inquiries requesting the College to respond with the name of the user that was on the network at the time the computer was performing certain actions. Sometimes these complaints come in the form of "Early Settlement Letters".
4. Baker College network officials forward these inquiries or letters to the supervisor of the identified user, or -- in the case of occupants of residence halls -- to the residence hall directors. Baker College will not release the name of the student or employee to the alleged copyright holder unless served with a proper subpoena, court order, or other legal process.
5. By forwarding these inquiries or letters to the supervisor or the hall director Baker College has made no determination as to whether the student or employee has engaged in copyright infringement, or that the user should enter into an early settlement with the copyright holder. Baker College believes that users should seek legal counsel before responding to these letters.
6. When the user has removed the offending P2P software the user's network access is automatically restored.
7. For more information please see <http://www.riaa.com/ispnoticefaq.php>

4.5 Incident Response

1. Violations of any of the above statements of policy may be indications of criminal offenses. Baker College students are required to report any instances where the violation of policies is occurring or has the potential to occur. The appropriate CIS Director is then charged with investigating the alleged violation. In order to prevent further possible unauthorized activity, CIS may suspend the authorization of computing services or telephone access to the individual or account in question. In accordance with established College practices, policies, and procedures, confirmation of unauthorized use of Baker College computer resources may result in disciplinary action.
2. Baker College CIS employees have a responsibility to provide service in the most efficient manner while considering the needs of the total user community. At certain times, the process of carrying out these responsibilities may require special actions or intervention by the staff. At all other times, CIS staff shall have no special rights above and beyond those of other users. CIS shall make every effort to ensure that persons in positions of trust do not misuse computing resources or data or take advantage of their positions to access information not required in the performance of their duties.
3. Baker College CIS employees prefer not to act as a disciplinary agency or to police activities. However, in cases of unauthorized, inappropriate, or irresponsible behavior, CIS does reserve the right to take remedial action, commencing with an investigation of the possible abuse. In this connection, CIS, with all due regard for the rights of privacy, shall have the authority to examine files, passwords, activity logs, accounting information, printouts, tapes, or other material that may aid the investigation.

5.0 Enforcement

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

6.0 Revision History

Adopted April 8, 2010

Revision Proposed October 28, 2010