

Technology Systems Usage Policy

BU-PP 025

Policy:

Baylor University provides information systems (including computers, computer accounts, printers, networks, dial-in systems, ResTech, software, electronic mail ("e-mail"), Web home pages, video systems, telephones, smart phones, telephone long distance and voice mail accounts) for the use of Baylor students, faculty, staff, and other authorized users, as approved, in support of the programs of the University.

Related Policies:

[BU-PP 029 — Handling of Confidential Information](#)
[BU-PP-023 — Standards of Personal Conduct \(political communication\)](#)
[BU-PP 705 — Faculty Dismissal Policy](#)
[BU-PP 807 — Staff Discipline Policy](#)
[Student Disciplinary Procedure](#)
[Web Site and E-mail Privacy Statement](#)
[Information Use Policy](#)

Additional Information: None

Contact:

Information Technology Services (254) 710-2711
Human Resources (254) 710-8539
Judicial Affairs (254) 710-1715

Technology Use

Baylor University technology systems [including computers, computer accounts, printers, networks, network devices, dial-in systems, ResTech, software, electronic mail ("e-mail"), Web home pages, video systems, telephones, smart phones, telephone long distance, and voice mail accounts] are provided for the use of Baylor students, faculty, staff, and other authorized users, as approved, in support of the programs of the University. All students, faculty, staff, and other authorized users are responsible for seeing that these technology systems are used in an effective, efficient, ethical, and lawful manner. The use of technology systems is a privilege, not a right, that may be revoked at any time for misuse.

1. The technology systems are owned by the University and are to be used for University-related activities only. All access to central technology systems, including the issuing of accounts, must be approved through Information Technology Services (ITS). All access to school and departmental information systems must be approved by authorized personnel within the respective departments.
2. Technology systems are to be used only for the purpose for which they are assigned. Incidental personal use of technology systems is permitted, but it must not interfere with the University's mission or official or educational use of such technology systems. Commercial use of Baylor's technology systems is prohibited.
3. Due to the possibility of technical failure, e-discovery or separation, faculty and staff are responsible for maintaining separate backups of personal files stored on Baylor University owned technology.
4. Electronic mail, voice mail, and files on a Baylor owned or Baylor operated technology system are presumed to be private and confidential unless they have explicitly been made available to other authorized individuals or as required by law. Their contents may be accessed only by authorized personnel for compelling University business or security reasons. All requests for electronic

records should be submitted to the information security officer or the vice president for information technology. The request must be accompanied by the approval of the president or the appropriate divisional vice president or their designee:

- a) for faculty members, the provost and executive vice president;
 - b) for staff members, the vice president for finance and administration;
 - c) for students, the vice president for student life; or
 - d) as required by law.
5. Fraudulent, harassing, offensive, or obscene messages or materials are not to be sent, printed, requested, displayed, or stored on Baylor-owned or operated technology systems. Information that invades an individual's privacy or is disparaging of an individual or business must not be published without the express consent of the person or business entity.
 6. To maintain information security and data integrity (backups), faculty's information for University-related academic business and for staff all work data must be stored on a Baylor owned technology resource.
 7. All forms of mass mailings, whether related to Baylor University or not, are prohibited without the prior approval of the divisional vice president.
 8. A computer, network resource, computer account, Web home page account, electronic mail account, ID card, or voice mail account assigned to an individual must not be used by others without the consent from the University provider of the resource. The individual is responsible for the proper use of the resource, including proper password protection.
 9. Technology system accounts that expire, along with the files in the expired accounts, may be deleted. Accounts expire in accordance with the terms of the account. E-mail and voice mail messages that are older than the limit set by the system administrator will be deleted.
 10. Software is installed on University technology systems in order to support resource usage accounting, security, network management, hardware and software inventory, computer back-up systems, and software updating functions and to provide better support to personnel. Authorized personnel may access others' files or systems when necessary for the maintenance of technology systems or when acting to protect performance, integrity, and security of technology resources. When possible, advanced notification of access will be given, except for cases covered by paragraph number three above. When performing maintenance, reasonable effort will be made to safeguard the privacy of a user's files. However, if violations of University policy or applicable law are discovered, they will be reported to the appropriate vice president or their designated representative.
 11. No one may attempt to degrade the performance of a technology system or to deprive authorized personnel of reasonable access to University technology systems.
 12. The use of loopholes or specific tools to circumvent technology systems or network security, the knowledge of special passwords, or the covert acquisition of passwords to damage technology systems, obtain extra resources, take resources from another user, or gain access or control of any system for which proper authorization has not been granted is expressly prohibited.
 13. Software and other materials that are protected by copyright, patent, trade secret, or another form of legal protection ("Protected Materials") may not be copied, altered, transmitted, or stored using Baylor-owned or operated technology systems, except as permitted by law or by the contract, license agreement, or express written consent of the owner of the protected materials. The use of software on a local area network or on multiple computers must be in accordance with the software license agreement.
 14. Baylor University may send official University correspondence to a student, faculty, or staff member via e-mail using the e-mail address assigned by Baylor. Each Baylor student, faculty, and staff member is personally responsible for checking his or her e-mail on a regular and recurring basis for receipt of official University correspondence.
 15. Baylor University contracts with a professional Web-filtering service to block sites that this vendor designates as adult content (e.g., obscenity, pornography). Additionally the same service is used

to block sites which pose information security risk to the University (e.g., phishing and malware sites). The ITS information security officer oversees a process to address misclassifications of content. Reclassification and the decision to block or unblock a site is at the University's discretion, and appeals should be submitted in writing to the vice president for information technology and dean of libraries.

SANCTION

An individual's technology systems usage privileges may be suspended immediately upon the discovery of a possible violation of this or other University policy. ITS may also disable accounts to protect the integrity of the information technology infrastructure or data stored within. The information security officer or vice president for information technology may authorize the disabling of an account for up to one business day. Such suspensions will be confidentially reported to the appropriate department head/chair, dean, ITS staff, and divisional vice president. An account may be disabled for longer than one business day by following the same approval process outlined in paragraph number three above.

The ITS administrative staff or supervising department head/chair will judge a violation of this policy as either major or minor. A first minor offense will normally be dealt with by the ITS administrative staff or supervising department head/chair. Appeals relating to minor offenses may be made to the appropriate vice president or his or her designated representative. Additional offenses will be regarded as major offenses. Major offenses will be dealt with by the appropriate vice president or his or her designated representative.

Violations of these policies by a faculty or staff member will be dealt with in the same manner as violations of other University policies and may result in a disciplinary review. A violation of this policy by a student may be referred to the Office of Judicial Affairs for discipline. In such a review, the full range of disciplinary sanctions is available, including the loss of technology systems usage privileges, dismissal from the University, and legal action. In some cases, violation of this policy may constitute a criminal offense under state or federal law.

DISCLAIMER

The Technology Systems Usage Policy and related policies may be revised from time to time. The latest official copy of this policy is available from the Information Technology Services and the Human Resources Web sites. Copies will also be posted on various University servers, such as the Baylor Web server. Other standards and guidelines (for electronic mail, Web pages, newsgroups, copyright, directory information, etc.) may be found on the Baylor Web server at: <http://www.baylor.edu/ITS/policies>.