Policy Title: Technology Usage Policy	**Policy Number: BU-PP-025**
Date Issued: January 2010	**Responsible Executive: Vice President of Information Technology**
Date Last Revised: May 2019	**Responsible Office: Information Technology Services**

Technology Usage Policy

Policy Statement

This policy addresses the intended use of technology for the Baylor University ("Baylor" or the "University") community.

Reason for the Policy

This policy sets forth the appropriate and inappropriate uses of Baylor technical resources.

Individuals/Entities Affected by this Policy

Who is affected by this policy

This policy applies to all active members of the University community, including faculty, staff, students, and affiliates, and to authorized visitors, guests, and others for whom a University technology resource or access to the network has been provided.

Technology affected by this policy

Baylor University technology systems (including, but not limited to, computers, computer accounts, internet, printers, networks, network devices, software, electronic mail ("email"), webpages, video systems, telephones, mobile devices, telephone long distance and voice mail accounts) are provided for the use of the University community in support of the programs of the University. The use of technology systems is a privilege, not a right, that may be revoked at any time because of misuse.

Exclusions

NONE

1. Technology Usage Policy

Related Documents and Forms

University Policies and Documents

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
Incident Response Policy
Network Usage Policy
Student Disciplinary Procedure
Website and Email Privacy Statement
Information Use Policy
Payment Card Industry Policy

Other Documents

- Family Educational Rights and Privacy Act (FERPA) 20 USC §1232g and 34 CFR Part 99
- Health Insurance Portability and Accountability Act (HIPAA) 42 USC §300gg and 1320d; 29 USC §1181 and 45 CFR Parts 146160, 162 and 164
- Gramm-Leach-Bliley Act 15 USC §6801 et seq and 16 CFR Part 313 et seq
- Fair and Accurate Credit Transactions Act (Red Flags Rule) 15 USC §1601 et seq
- Protection of Human Subjects Regulations ("Common Rule") 45 CFR Part 46
- Texas Business and Commerce Code privacy laws Tex. Bus. & Comm. Code Chapters 501-503
- Privacy Act of 1974 5 USC §552a et seq
- Texas Public Information Act Texas Government Code Chapter 552
- Children's Online Privacy Protection Act (COPPA) 15 USC §6501 et seq and 16 CFR Part 312
- European Union General Data Protection Regulation (EU GDPR) EU 2016/679
- PCI DSS

Definitions

These definitions apply to terms as they are used in this policy.

Baylor University Technology Systems	Baylor-owned, licensed, or operated technology systems including, but not limited to, computers, computer accounts, internet, printers, networks, network devices, software, electronic mail ("email"), webpages, video systems, telephones, mobile devices, telephone long distance and voice mail accounts that are provided for the use of University community in support of the programs of the University
E-Discovery	Refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format
Incidental Personal Usage	Incidental personal use of University technology resources is permitted; as long as the personal use: • Results in no additional cost to the University • Is minimal in time and duration • Does not interfere with job responsibilities • Are not prohibited activites
ITS	Information Technology Services
Protected Materials	Software and other materials that are protected by copyright, patent, trade secret, or another form of legal protection
University Community	Faculty, staff, students, affiliates, authorized visitors, guests, and others for whom a University technology resource or access to the network has been provided

Contacts

Subject	Contact	Telephone	Office email/web site
Policy Management	Information Technology Services	254-710-2711	www.baylor.edu/its
Employment Concerns	Human Resources	254-710-2000	askHR@baylor.edu
Student Concerns	Student Conduct Administration	254-710-1715	www.baylor.edu/studentconduct

Responsibilities

University President or Designee	The University President may approve authorization and/or exceptions requests from faculty, staff, or students.
Provost or Designee	To approve authorization and/or exceptions requests regarding faculty members
Vice President and Chief Human Resource Officer or Designee	To approve authorization and/or exceptions requests regarding staff members
Vice President of Student Life or Designee	To approve authorization and/or exceptions requests regarding students
ITS Chief Information Security Officer or Designee	Responsible for developing and implementing an information security program to ensure that University communications, systems, and assets are safeguarded from threats
Chief Information Officer or Designee	Responsible for ensuring the policy remains current and for managing the application of the policy

Principles

Proper Use of Technology

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 with official or educational use of such technology systems. If University technology is used for personal reasons, the individual must acknowledge:

- The University assumes no responsibility to backup or to assist in recovery of personal information.
- Individuals are personally responsible for backing up all personal information to non-University technology systems.

- When personal information is stored on University technology systems, such information is subject to University policy and practice, including important limitations in the privacy of such information

Individual Accountability

The University provides individual accounts to access University technical resources. The individual is responsible for the proper use of the technical resources, including mobile devices. The individual account information and password should never be shared.

Adherence with Federal, State, and Local Laws

All members of the University community are expected to uphold, federal, state, and local laws:

- Abide by all applicable federal, state, and local laws
- Abide by all applicable copyright laws and licenses. Baylor University has entered into legal agreements or contracts for many of our software and network resources, which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts, and other media both in personal use and in production with electronic information.
- Do not use, copy, or distribute copyrighted works (including, but not limited to, webpage graphics, sound files, film clips, trademark, software, and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation, and/or criminal prosecution.
- 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, licensed, 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.

Prohibited Activities

The following list is not intended to be all-inclusive.

- Uses that could jeopardize the University's 501(c)(3) federal tax-exempt status
- Uses for political purposes
- Uses for self-employment opportunities
- Uses for a purpose other than their intended purpose
- Uses that are unethical and not reflective of the University's Christian mission

- Fraudulent, harassing, offensive, or obscene messages or materials are not to be sent, printed, requested, displayed, or stored on Baylor-owned, licensed or operated technology systems.
- Information that invades or abuses 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.
- No one may attempt to degrade the performance of a technology system or to deprive authorized personnel of reasonable access to University technology systems.
- The use of loopholes or specific tools to circumvent technology systems or network security, the use 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.
- Failing to protect sensitive or mission critical information. It is each individual's responsibility to take steps to safeguard sensitive information.
- Destruction of University data must be properly approved and follow University policy or departmental procedures.

Email and Communication

Baylor University may send official University correspondence to a student, faculty, or staff member via email using the email address assigned by Baylor. Each Baylor student, faculty, and staff member is personally responsible for checking his/her email on a regular and recurring basis for receipt of official University correspondence.

All forms of mass mailings, whether related to Baylor University or not, are prohibited without the prior approval of the appropriate divisional vice president.

Incident Response

ITS security staff should be notified immediately of any suspected or confirmed security incident involving Baylor technology assets or University data. Please refer to the Incident Response Policy for more details concerning reporting security incidents.

University Technical Services

- **Technology Ownership -** The technology systems are owned, licensed, or operated by the University and, except as specifically permitted in this policy, are to be used for University-related activities only. All access to central technology systems, including the issuing of accounts, must be approved through ITS. All access to school and departmental information systems must be approved by authorized personnel within the respective departments.
- **Data Integrity -** To maintain information security and data integrity, faculty's information for University-related academic business and all work data for staff

must be stored on a Baylor-owned, licensed, or operated technology resource. 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 or in compliance with court orders or other legal requirements. When possible, advanced notification of access will be given, except for cases covered by Exceptions/Approvals. 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 the appropriate authorities.

- **Data Backup -** ITS provides centralized backups for faculty and staff primary computers. 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.
- **Access and Data Expiration -** 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. Email and voice mail messages that are older than the limit set by the system administrator will be deleted.
- **Content Restriction -** Baylor University contracts with a professional web-filtering service to block sites the vendor designates as adult content (e.g., obscenity, pornography). Additionally, the same service is used to block sites which pose an information security risk to the University (e.g., phishing and malware sites). The ITS Chief 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.

Exceptions/Approvals

Electronic mail, voice mail, and files on a Baylor-owned, Baylor-licensed, 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 Chief 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:

- for faculty members, the Provost;
- for staff members, Vice President and Chief Human Resources Officer;
- for students, the Vice President for Student Life; or
- as required by law.

Sanctions

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 chief 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 Exceptions/Approvals.

The ITS administrative staff or supervising department head/chair may judge some violations 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. Additional offenses will be regarded as major offenses. Major offenses will be dealt with by the appropriate vice president. Questions regarding the severity of the offense can be addressed to the chief information security officer for clarification.

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 Student Conduct Administration 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, in which case the proper authorities will be notified.

Disclaimer

The senior management and ITS positions mentioned within this policy may assign their responsibility to a designee. The Technology Systems Usage Policy and related policies may be revised on an as needed basis. The latest official copy of this policy is available from the Information Technology Services and the Human Resources websites. Copies will also be posted on various University servers, such as the Baylor Web server. Other standards and guidelines (for electronic mail, webpages, newsgroups, copyright, directory information, etc.) may be found on the Baylor Web server at: **www.baylor.edu/ITS/policies.**