Baylor University

Policy Title: Information Use Policy	**Policy Number:**
Date Issued: August 2007	**Responsible Executive: Vice President of Information Technology**
Date Last Revised: April 2, 2020	**Responsible Office: Information Technology Services**

Information Use Policy

Policy Statement

Baylor University ("Baylor" or the "University") collects, stores, and uses data and information via information technology systems. Employees shall not access, acquire, use, copy, or transfer confidential information except to the extent reasonably necessary to fulfill their employment duties.

Reason for the Policy

Baylor is committed to safeguarding confidential information. During your relationship with Baylor, you may have access to confidential information. This policy assists with the identification and proper access of confidential information to ensure its privacy and integrity.

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, vendors, 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, and telephone long distance and voice mail accounts) are provided for the use of the University community in support of the programs of the University.

Exclusions

NONE

Related Documents and Forms

University Policies and Documents

Technology Systems Usage Policy
Directory Information Policy
Employee Personal Information
Handling of Confidential Information
Student Policies & Procedures
Network Usage Policies
Password Policies
Server Security Policy
Incident Response Policy
Data Classification Guide
Departments Authorized to Release Information
FERPA Policy

Forms and Tools

Forms and tools are available at www.baylor.edu/its/.

Definitions

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

Confidential Information	Confidential information is defined as non-directory information pertaining to students, alumni, employee records, University financial records, trade secrets, and any other information maintained in a confidential manner according to University policy or practice. Such confidential information may include, for example, academic records, compensation, and other financial information.
Information Technology System	Information technology systems are defined as Baylor University owned systems that transmit or store University data. These may include, but are not limited to, computers, computer accounts, printers, networks, network devices, dial-in systems, software, electronic mail, web homes pages, video systems, telephones, and telephone long distance and voice mail accounts.
University Data and Information	For the purposes of this policy, University data and information includes directory information (as defined in the Directory Information Policy and the Student Policies and Procedures) and non-directory information. Non-directory information would include most non-public information stored in the various student, alumni, financial, human resources, and ancillary systems operated by the University. This policy is not intended to establish ownership rights for materials or intellectual property produced by students, faculty, staff, or others that utilize the University's systems.

Contacts

Subject	Contact	Telephone	Office email/web site
Support	ITS Help Desk	254-710-4357	https://www.baylor.edu/its/index.php?id=44608

Responsibilities

Chief Information Officer	The Chief Information Officer has the responsibility of overseeing Social Security number usage on campus.
Employees	With respect to data and information, employees will: 1) Employ reasonable and appropriate security technology and practices to safeguard the information stored in University technology systems; 2) Use the information stored and collected in the University's technology systems for the purposes of the University; 3) Not release confidential information to the public or to non-related third parties unless required by law or other legal proceedings or with permission from the affected party(ies). Employees shall take all appropriate action to ensure the protection, confidentiality, and security of confidential information. The obligation of an employee to maintain the confidentiality and security of confidential information survives the termination of employment with the University.

Principles

Handling of Confidential Information

During the course of their employment, employees may encounter confidential information, particularly through the use of University computing facilities. Employees shall not access, acquire, use, copy, or transfer confidential information except to the extent necessary to fulfill their employment duties. All other individuals who are authorized to access or use confidential information of the University may only access, acquire, use, copy, or transfer such confidential information in a manner specified by and consistent with the University's authorization.

Access to and disclosure of student educational records are governed by regulations promulgated under the Family Educational Rights and Privacy Act (34 C.F.R. 99.1 et seq.) and by the Directory Information Policy. Generally, any information concerning the educational records of a student cannot be disclosed to any other party without the prior written consent of the student. Specific questions concerning under what conditions information about a student may be obtained or disclosed should be directed to the Academic Records division in the Office of the Registrar.

Access to and disclosure of student, employee, donor, and financial records is governed by the Handling of Confidential Information Policy and the Employee Personal Information Policy. After reviewing these policies, any questions concerning under what conditions information about an employee may be obtained or disclosed should be directed to the Personnel/Payroll Office.

Employees shall take all appropriate action to ensure the protection, confidentiality, and security of confidential information. The obligation of an employee to maintain the confidentiality and security of confidential information survives the termination of employment with the University.

Directory Information

Faculty, staff, and student (current and former) directory information is made available through information technology systems. Various systems provide name, address, phone number, and email address.

The Directory Information Policy is the policy guiding all usage of directory information on campus. Utilization of all directory information is restricted to University business. This information will not be released to non-related third parties. Requests from outside of the University for information about employees must be referred to the Personnel/Payroll Office. Requests from outside of the University for information about students must be referred to the Academic Records division of the Office of the Registrar.

Social Security Numbers Guiding Philosophy

With respect to Social Security numbers, the University is guided by the following objectives:

1) Broad awareness of the confidential nature of the Social Security number;
2) Reduced reliance upon the Social Security number for identification purposes;
3) A consistent approach regarding the use of Social Security numbers throughout the University; and
4) Increased confidence by students and employees that Social Security numbers are handled in a confidential manner.

UIN/Social Security Number Usage

1) A University-wide Unique Identification Number (UIN) is assigned to all students, employees, and other associated individuals, such as contractors or consultants. The UIN will be considered a public piece of information. This UIN will be assigned at the earliest possible point of contact between the individual and the University. The UIN will be used in all future electronic and paper data systems to identify, track, and service individuals associated with the University. It will be permanently and uniquely associated with the individual to whom it is originally assigned.

    a. The UIN will be considered the property of Baylor University, and its use and governance shall be at the discretion of the University, within the parameters of the law;
    b. The UIN will be maintained and administered by Information Technology Services (ITS);
    c. The UIN will be a component of a system that provides a mechanism for both the public identification of individuals and a component of authentication.

2) Grades and other pieces of personal information will not be publicly posted or displayed in a manner where either the UIN or Social Security number identifies the individual associated with the information.

3) Paper and electronic documents containing Social Security numbers should be disposed of in a secure fashion.

4) Except where the University is legally required to collect a Social Security number, individuals will not be required to provide their Social Security number, orally or in writing, at any point of service, nor will they be denied access to those services should they refuse to provide a Social Security number. However, individuals may volunteer their Social Security number if they wish as an alternate means of locating a record or authentication.

5) The Social Security number may continue to be stored as an attribute associated with an individual. The Social Security number may be used as needed to identify individuals for whom a UIN is not known.

6) This policy does not preclude, if a primary means of identification is unavailable, Baylor University employees from using the Social Security number as needed during the execution of their duties. The University is also permitted to continue to collect Social Security numbers in a manner consistent with state and federal law.

7) The Chief Information Officer has the responsibility of overseeing Social Security number usage on campus. This administrator will control the Social Security number and his/her approval will be required to collect, use, or store Social Security numbers in any existing or new electronic system.

Sanctions

Sanctions may include, but are not limited to, suspension of technology privileges, termination of employment, referral to Student Judicial Services, and/or criminal prosecution. For additional information, please reference the Technology Systems Usage Policy.

Persons who exceed their authority in using confidential information or who gain access to such information through unauthorized means, including the use of University computing facilities, should realize that their conduct is in violation of University policy and will be dealt with accordingly. Such conduct may also be in violation of state and federal law and may subject such persons to penalties of fines or imprisonment or both.