Privacy of Personal Information

**Purpose**
The University is committed to protecting the privacy of its students, employees and visitors within its control in a manner consistent with applicable laws, regulations, and University policies. To help achieve this, the University has adopted a “privacy by default” model. Consideration for business effectiveness and efficiency must be carefully weighed against increased privacy restrictions.

This standard provides guidance for the appropriate collection and use of personal information, including its use in public and internal directories, information systems and websites, to ensure privacy objectives are achieved.

For additional information or questions, contact the BYU Privacy Officer (privacy@byu.edu).

**Definitions**
Personal Information (PI) – Any information, including contact information, which relates to or is associated with, describes, identifies, or can be reasonably used to identify a natural, living person.

Public Directory – Any list containing the names and/or other PI of faculty/employees that is assessable to the public (student names and/or their corresponding PI is not included as part of Public Directory).

Internal Directory – Any list containing the names and/or other PI of active faculty/employees or students (if such students choose to opt-in) that is assessable to the general campus community (faculty/employees, adjunct faculty, contractors and students).

Internal – Information generally accessible within the University to those with a legitimate business need (cf. internal security classification).

**Applicability**
This standard applies to all university departments, faculty, staff, employees, consultants, and third party service providers.

**Privacy Standard**
PI should only be obtained through lawful means and is permitted to be used by employees and contractors to provide educational related services without consent, as defined in the BYU Privacy Notice. If non-public PI is to be accessed or shared with third parties, they should be bound by contract to abide by the University’s privacy and security policies, standards and agreements. Consent should be received by data subjects before their PI is
collected or used for purposes outside the scope of the BYU Privacy Notice or other applicable notices provided at the time of collection. The following privacy principles provide guidance to protect the PI we collect, use and store:

- **Notice** – The purpose for collecting PI is described at the time it is collected and is not used for secondary purposes not described in the notice. Notice is normally provided by placing a link to the BYU Privacy Notice in website footers or in easily visible locations on data entry screens;
- **Consent** – An individual’s explicit consent is required when collecting, using, or sharing personal information for purposes outside the scope of the BYU Privacy Notice. Explicit consent is clear and easily understood, is freely given and specific to the purposes described. Consent can be revoked for any reason, at which time, the individual’s personal information is deleted;
- **Privacy by Default** – Deliver the maximum degree of privacy by ensuring that PI is automatically protected by default. Individuals need not opt-out nor do anything to keep their PI intact. Individuals can opt-in to allow additional PI to be disclosed to others;
- **Minimization** – Only collect or use PI that is necessary to complete legitimate business purposes. Avoid requesting or collecting unnecessary PI, e.g., only collect the SSN or DOB when necessary;
- **Access** – Access to PI is limited to those faculty/employees with a legitimate business need, in order to perform their job functions;
- **Accuracy** – Take steps to ensure the accuracy, completeness and relevance of PI;
- **Protection** – Ensure Minimum Security Controls are in place to safeguard personal or confidential information from reasonably anticipated risks, such as loss, unauthorized access, use, modification, disclosure or deletion. The loss of PI is reported without undue delay to SOC;
- **Sharing** – PI is not shared outside the organization without appropriate agreements in place. A Data Sharing Agreement (DSA) and/or a Data Privacy & Security Addendum is executed before PI is shared. Vendors can demonstrate compliance with processing obligations by providing proper documentation to BYU or a supervisory authority upon request;
- **Data Subject Requests** – When allowed by law, fulfill data subject requests to view, receive a copy of, correct or delete their PI. PI subject to retention requirements can only be deleted when the applicable retention period has been met;
- **Retention** – PI is retained in compliance with BYU Policy and the General Retention Schedule (GRS), in order to comply with legal obligations, meet operational needs, and provide evidence of business decisions and transactions;
- **Deletion or De-identification** – PI is stored for no longer than is necessary to complete the purposes for which it was collected. PI is either deleted or de-identified when its business purpose has been met.

**Biometric and Genetic Data**

Individuals can be identified through various types of biometric authentication information, including fingerprints, facial recognition, retinal scans, x-ray images and gene sequences. Given the sensitivity of this data, notice and consent is required when collecting, using or sharing biometric or genetic data of an individual.

**Public Directory**

- **Faculty/employees** – By default, limit the contact information of faculty/employees to what is necessary for people outside of BYU to identify and make contact with faculty/employees. By default, the Public Directory for faculty/employees may display their, name, photo, title, department and the department’s main address, phone number and email address, with the ability for faculty and employees to opt-in to display additional contact information, including their direct office address, direct office phone number, cell phone number, and direct email address. Faculty/employees cannot opt-out of the default contact information from being displayed.
• **Students** – The Public Directory should not display any student contact information.

**Internal Directory**
The Internal Directory is to be classified as Internal and is only visible to current students, faculty, adjunct faculty, employees, and contractors that are logged in through BYU’s Central Authentication System (CAS) or other approved methods. The Outlook Global Address List and other similar system directories used across campus, such as Box, Zoom, etc., may display the Net ID@byu.edu and other necessary login information to enable users to communicate to one another for work or educational related purposes. When listing students, these directories should not contain additional contact information.

• **Students** – Student PI is unlisted by default. Students must opt-in to display their contact information to other students found in Internal Directories. Unlisted student records and their associated PI will not be available to third parties, but will be visible to current faculty/employees with a legitimate educational interest.

• **Restricted students** – Students should have the option to restrict their records, making their contact information, including name, unavailable to the Internal Directory. Restricted records will continue to be made available to employees with a legitimate educational interest. Students will need to interact with the Registrar’s Office to restrict their records.

• **Faculty/employees** – The name, photo, work email address, direct work address and direct phone number should be made to the Internal Directory, by default, without the ability to opt-out, as it will make it difficult for faculty/employees to work with one another and for students to access campus resources. Faculty/employees can opt-in to display additional contact information.

• **Restricted faculty/employees** – Faculty/employees cannot restrict their direct work contact information from the Internal Directory. When taking classes, faculty/employee directory information will default to showing only their work contact information, if they have done a “FERPA” restriction through the Registrar’s Office.

• **Student Employees** – Students requiring access to PI beyond what is accessible in the Internal Directory may receive appropriate access by completing the official campus FERPA training and then having their full-time supervisor request access. Access to PI will be limited to legitimate business needs.

**Public Department Websites**
Departments may provide public access to their faculty/employee information on BYU department websites, as long as they comply with the rules outlined in the Public Directory above. No student, student employee or former student contact information should be listed on the public area of department websites without prior consent from the individual.

**Printed Directories**
Printed directories created by BYU or its departments contain personal information and therefore should be restricted for campus use only. Printed directories should follow the same rules as the Internal Directory above. Printed directories should be labeled as “Internal Use Only” and securely disposed when no longer needed.
Related Information

- Information Governance Standards and Procedures
- Information Security Standards and Procedures