INFORMATION PRIVACY STANDARD
Privacy of Personal Information

Procedure Contents
• Related Policy
• Purpose
• Applicability
• Privacy Standard
• Related Information

Effective Date: NEW DRAFT
Last Updated: 
Responsible University Officer: 
VP Technology/CIO
Owner: 
Chief Information Security Officer
Contact: 
Tracy Flinders

RELATED POLICY: Information Security and Appropriate Use

Purpose
The University is committed to protecting the privacy of the personal information of its students, faculty, and staff 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 on the appropriate collection and use of personal information, including the use of personal information in public directories and websites, to ensure privacy objectives are achieved.

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

Applicability
This standard applies to all university departments, faculty, staff, employees, consultants, and third party service providers. If non-public personal information is to be accessed or shared with third parties, they should be bound by contract to abide by the University’s Information Security and Appropriate Use Policy.

Privacy Standard
In general, personal information is not to be made available to the public nor shared with outside organizations without a lawful basis or the opt-in consent of the data subject. Appropriate standards and procedures should be implemented to ensure

• only authorized individuals can access, alter, disclose, or destroy personal information;
• individuals are allowed to act only within the scope of their authority;
• personal information is adequately protected from inappropriate use, loss, alteration, or destruction, and can be recovered to prevent damage or distress to the individuals concerned;
• data breaches are reported without undue delay;
• only collect the personal information required to perform the necessary business purpose and securely dispose of the personal information when it is no longer needed
• requests by data subjects regarding what data we are processing and obtaining a copies are properly fulfilled; and
• vendors can demonstrate compliance with processing obligations by providing proper documentation to BYU or a supervisory authority upon request.
Public Directory Information

- **Faculty/Employees** – by default, limit personal information of faculty and employees to what is necessary for people inside and outside of BYU to make contact, including potential, current and prior students, faculty and employees. By default, the public directory should display name, title, department and the department’s main address, phone number and email address, with an easy way for faculty and employees to opt-in to display additional personal information, including individual office address, phone number and email address, as well as their home address and phone number, in case they want to be found more easily.

- **Students** – Our public directory should not display any student information. Student information should only be made available behind our general login, only available to active faculty, employees and students.

BYU Campus Community Directory for Current Students, Faculty and Employees

The BYU Campus Community Directory is to be classified as “Internal” and only visible to current students, faculty (including adjunct faculty), employees, and contractors with an appropriate role and logged in through BYU’s Central Authentication System (CAS).

- **Students** – student directory information will be unlisted (only the student’s name will be visible by other students) by default. Students will need to opt-in to display their personal contact information in the campus community directory to other students, with options for what information to display. Unlisted student records will not be available to third parties, but will still be visible to current faculty/employees.

- **Restricted student records** – Students should have the option to restrict their records, making their personal information, including name, unavailable to the general campus community and third parties. Restricted records will continue to be made available to managers/leaders with a legitimate educational interest. Students will need to interact with the Registrar’s Office to restrict their records.

- **Faculty/Employees** – name, picture, work email address, department, office address and phone number should be made available by default, with no ability to opt-out. Opting out of any of these fields would make it difficult for faculty/employees to work with one another. Faculty/Employees should have the ability to opt-in to display home address and personal phone number/cell phone.

- **Restricted faculty/employee records** – Faculty and employees should not have the ability to restrict their records from the community directory. When taking classes, faculty/employee directory information will default to showing only their work information if they have done a “FERPA” restriction through the Registrar’s Office.

Public Department Websites

Departments may provide public access to department information on BYU department websites, including a listing of faculty, with contact information limited to name, photo, title, office address/phone, and work email address. However, the default should be work address, phone, and email of the department and not of the faculty/employee. Faculty/employees should have the right to choose whether their work contact information
displays on the public department sites or whether the department’s main address, email and phone display on the website.

No student or student employee personal data should be listed on the public area of department websites without prior student consent.

**Printed Directories**
Printed directories, such as the BYU Telephone Directory, should be restricted for campus use and should follow the same rules as the BYU Campus Community Directory above. Printed directories should be labeled as “Internal Use Only” and securely disposed of when no longer needed.

**Related Information**
- Information Governance Standards and Procedures
- Information Security Standards and Procedures