Information Privacy and Compliance Training

For all BYU–Idaho Employees
BYU-Idaho considers maintaining the security and confidentiality of PRIVATE INFORMATION a matter of highest priority. Many employees and contractors are granted or have access to private information, and all employees and contractors are required to agree in writing that they will preserve the security and confidentiality of this information.
Objective

This training is provided to ensure that all employees have a basic understanding of the policies and laws that govern the privacy of information to allow them to meet their obligation to maintain the confidentiality of private information.
The privacy laws and standards the University is required to comply with include, but are not limited to:

- Family Education Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Fair and Accurate Transactions Act (FACTA)
- Health Insurance Portability and Accountability Act (HIPAA)
- PCI DSS – Credit Card Standards
FERPA specifically protects the privacy of all records of individual students. While there are certain exceptions, employees should not share student information with anyone other than the student, without consulting the Student Records and Registration Office. (This does not include information shared with other employees in the process of fulfilling job duties.)
GLBA protects any record containing nonpublic FINANCIAL information about a student or any third party who has a relationship to the University.
FACTA requires efforts to detect and prevent identity theft, particularly as it relates to personal accounts (BYU-Idaho accounts receivable) by defining and monitoring indicators of identity theft that are referred to as “red flags”.
RED FLAGS include, but are not limited to:

- Alerts, notifications, or warnings from a consumer reporting agency.
- Notice from an account holder that they are victims of identity theft.
- Presentation of suspicious identification documents to any BYU-Idaho administrative office.

RED FLAGS should be reported to the University Bursar at (208) 496-1920.
HIPAA applies to any medical records (including mental health records) that are in the possession of the University. While this applies primarily to the STUDENT HEALTH CENTER and the STUDENT COUNSELING CENTER, others may occasionally have access to such information and are required to protect it.
Departments, third parties, or computer programs that accept credit card payments must comply with PCI-DSS.

Avoid writing down credit card information. If writing is necessary, destroy the written material as soon as possible. Never store credit card data on a computer except as part of an approved card processing system.
DIRECTORY INFORMATION may be shared, unless restricted by the student. This information includes:

- Name
- Addresses
- Phone numbers
- Dates of attendance
- Major field of study
- Degrees and awards
- Previous educational institutions attended
- Graduation date
- Class schedule
- Pictures
- Period of enrollment
- Class standing
- Enrollment status
- Deferred registration eligibility

The University is permitted to release directory information without written consent from the student, according to established University procedure. For more information, please contact the Student Records and Registration office at (208) 496-1002.
Some individuals have requested their DIRECTORY INFORMATION not be shared. Notification is displayed on computer screens when this is the case. For third party inquiries regarding these individuals, the proper response is: “I have no information to share on that individual.”
Information about a particular individual that is **not** listed as **DIRECTORY INFORMATION** on the previous pages **is considered private**.

Exceptions must be approved by the Director of Financial Services (for financial information), by the Health Center Administrator (for medical information), and by the Registrar (for other student information).
All FACULTY and many OFFICE ASSISTANTS and STUDENT EMPLOYEES have access to protected FERPA information; and privacy violations can happen unless care is taken. Some specific “do’s and don’ts” include:
Do not:

• Leave graded papers out in view.
• Leave grade lists with student identification information in view (remember, others may have access to your office for ecclesiastical or janitorial purposes).
• Give out PRIVATE INFORMATION over the phone.
• Give PRIVATE INFORMATION to spouses or parents without written signed authorization (or proof of dependency on the part of parents).
Do’s and Don’ts

Do:

• Request proof of ID before providing student information.
• Shred tests and other documents that include student information and grade information.
• Require all employees with access to private information to take this training.
Information that does not include PERSONALLY IDENTIFIABLE DATA (i.e. data that would connect that information to an associated name) is not protected.

(Examples of identifying information include: name, social security number, user name, or other information that would make determining an individual’s identity possible.)
SUMMARY or STATISTICAL data (i.e. information that is NOT tied to identifying information) is not protected by law. However, any such data should only be made public by the department or individuals authorized to do so. In most instances, this will be done through the University Relations office or in specific publications.
Any information that has been published in a medium available to the general public may be shared without restriction.
Protected information must be secured, irrespective of the medium, whether:

- Paper
- Electronic
- Any other form
Unsecured Server Storage

- Do not store private information on a public web server (e.g. BYU-Idaho web servers, Dropbox, Carbonite, Google Docs, etc.) that might be subject to discovery and access using an internet search engine.
- Personally Identifiable Information (PII) (including students’ grades) must be stored in a secure location.
- If you have questions about where you can securely store PII, please contact the Information Technology office at (208) 496-7000.
Email lacks the security necessary to protect private information. Such information can only be sent by email if it is within an attached file that is password encrypted.
Confidential information stored on a PORTABLE ELECTRONIC DEVICE such as a laptop, USB drive, CD, DVD, or smart phone should be encrypted to ensure data cannot be retrieved by an unauthorized person if the device is lost or stolen. For questions regarding encryption, contact the Information Security Officer at (208) 496-7012.
BYU-Idaho user names and passwords should not be shared. Passwords should be changed regularly and when it is suspected they have been compromised. Passwords should use a combination of upper and lower case letters, numbers, and special characters and should not be words or names.
Protected information may be shared with others in the performance of an individual’s authorized duties. Such information should NOT be shared with those who have no official need for the information.
One may have rights to certain private information. However, unless the information is needed in the performance of employment duties, it should NOT be accessed. For example, accessing private information to accommodate ecclesiastical needs is not appropriate.
Generally, information may NOT be shared with parents of students, unless the student has given specific written authorization to share such information. Requests for student educational records should be directed to the Student Records and Registration Office. Requests for financial information should be directed to the Financial Services Office. Requests for student health information should be directed to the Student Health Center.
Each department is responsible for ensuring compliance with privacy laws and should have processes in place for securing private information. These processes should include securing computers by protecting passwords and LOCKING or LOGGING OUT of computers when leaving a work area.
Each department should have secure processes to **ensure** that any **printed material containing private information** is **handled and stored appropriately**. Such information should not be in public view, left in unsecured offices, and should be stored in locked files after business hours.
Placing protected information in an unsecured garbage bin (including blue recycle bins) is not an acceptable method of disposal for documents that contain private information. **Such information should be secured until shredded or properly destroyed.** For small volumes, a department shredder should be sufficient. Departments with large volumes should contact the Custodial Manager (ext. 2500) for details regarding the BYU-Idaho secured storage and disposal contract.
Electronic data containing private information should be destroyed in such a way that the information is not subject to retrieval. Data on disks that has been deleted or even reformatted can still be retrieved. The storage device should either be physically destroyed or erased by a reliable program that overwrites the device with multiple passes. For questions call Information Technology at ext. 7000.
In the course of their employment, employees may occasionally find themselves in a position to access private information to which they are not authorized. Employees shall avoid accessing such information.
Because of the significant risk to the University and its students and other patrons, violation of privacy policies may result in termination of employment. Violations should be reported to the Financial Services Director (ext. 1901) or anonymously on the BYU-Idaho Compliance Hotline at 1 (888) 238-1062.
Unauthorized Access or Attempt to Gain Access

Any employee who observes what appears to be unauthorized access or attempted unauthorized access to electronic information or similar electronic security breach or suspicious activities should notify the Information Security Officer at ext. 7012.

Non-electronic unauthorized access or attempted access should be reported to the Financial Services Director or Internal Auditor at ext. 1901.
A policy or procedure cannot be written to cover every privacy issue that might arise on campus. We expect all employees to exercise good judgment in protecting private information. When in doubt of what to do, please consult with your supervisor.