
BRIGHAM YOUNG
UNIVERSITY
IDAHO

BRIGHAM YOUNG UNIVERSITY IDAHO

Privacy and Information Security Training

For all BYU–Idaho Employees

BRIGHAM YOUNG UNIVERSITY IDAHO

Overview

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Laws

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

BRIGHAM YOUNG UNIVERSITY IDAHO

FERPA

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.)

BRIGHAM YOUNG UNIVERSITY IDAHO

GLBA

GLBA protects any record containing nonpublic FINANCIAL information about a student or any third party who has a relationship to the University.

BRIGHAM YOUNG UNIVERSITY IDAHO

FACTA

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”.

BRIGHAM YOUNG UNIVERSITY IDAHO

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

HIPAA

HIPAA applies to 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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Payment Card Industry - Data Security Standard (PCI DSS)

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Directory Information

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Special Restrictions

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.”

BRIGHAM YOUNG UNIVERSITY IDAHO

Non-Directory Information

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).

BRIGHAM YOUNG UNIVERSITY IDAHO

Specific FERPA Considerations

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:

BRIGHAM YOUNG UNIVERSITY IDAHO

Do's and Don'ts

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).

BRIGHAM YOUNG UNIVERSITY IDAHO

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Non-Private Information

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, username, or other information that would make determining an individual's identity possible.)

BRIGHAM YOUNG UNIVERSITY IDAHO

Summary Data

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Published Information

Any information that has been published in a medium available to the general public may be shared without restriction.

BRIGHAM YOUNG UNIVERSITY IDAHO

Information Medium

Protected information must be secured, irrespective of the medium, whether:

- Paper
- Electronic
- Any other form

BRIGHAM YOUNG UNIVERSITY IDAHO

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 accessible or searchable using an internet search engine.
- Personally Identifiable Information (PII) (including students' grades) must be stored in a secure location.
- If you have questions about properly securing information, please contact the BYU-Idaho Support Center at (208) 496-1411 or visit the IT website.

BRIGHAM YOUNG UNIVERSITY IDAHO

Email

Private information should not be sent through email. Email lacks the security necessary to protect private information. Such information can only be sent by email within an attached file that is password-encrypted.

BRIGHAM YOUNG UNIVERSITY IDAHO

Phishing Emails

- Be cautious when opening emails that include attachments or embedded links. Many devices and systems are compromised when users open suspicious attachments or click on questionable links within an email. Verify embedded links for authenticity before clicking on them.
- Emails requesting your personal information may not be legitimate. Consider the source of the email and do not click on any links that do not seem authentic.
- If you have questions about phishing emails or would like to report a phishing email scam, please contact the BYU-Idaho Support Center at (208) 496-1411 or visit the IT website.

BRIGHAM YOUNG UNIVERSITY IDAHO

Social Engineering

- Social engineering is the act of manipulating individuals in order to obtain confidential or secure information. For example, an individual may contact you through email or phone and ask you for billing or specific account information. Do not give out any confidential information without authorization.
- Criminals may also try to impersonate authority figures in order to gain access to restricted areas. Verify the authenticity of these persons before allowing them into restricted areas or providing them with confidential information.
- If you have any questions or concerns, please consult your line management or contact the BYU-Idaho Support Center at (208) 496-1411.

BRIGHAM YOUNG UNIVERSITY IDAHO

Viruses and Malware

- Antivirus software has been installed on every computer to scan and protect against virus and malware attacks. To ensure the safety and security of your computer, do not disable the antivirus software.
- Do not install antivirus software from unauthorized sites. For BYU-Idaho recommended software, visit the IT website.
- If you suspect a virus on your computer, please contact the BYU-Idaho Support Center at (208) 496-1411.

BRIGHAM YOUNG UNIVERSITY IDAHO

Protecting Electronic Data

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.

If you have questions about encryption, please contact the BYU-Idaho Support Center at (208) 496-1411 or visit the IT website.

BRIGHAM YOUNG UNIVERSITY IDAHO

Password Protection

BYU-Idaho usernames and passwords should not be shared. Passwords should be changed regularly or when they may have been compromised. Passwords should use a combination of upper and lower case letters, numbers, and special characters. Do not use full words or names in a password.

BRIGHAM YOUNG UNIVERSITY IDAHO

Information Sharing

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Right to Know vs. Need to Know

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Parents

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Protecting Information

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Record Handling and Storage

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Record Disposal

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Disposal of Electronic Data

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Unauthorized Information Access

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Policy Violations

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

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.

BRIGHAM YOUNG UNIVERSITY IDAHO

Conclusion

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.