Data Use, Privacy, and Security Policy

As an institution where "a commitment to excellence is expected" (BYU Mission Statement), Brigham Young University strives to maintain standards and practices that accord with ethical, contractual, and legal requirements for data use, privacy, and security.

Definitions

Data Sharing Agreement means a formally recorded document created through campus data governance procedures that describes the use case and data resources needed to share university data with specific parties.

Data Steward means an employee with designated responsibility for processing a specific set of data.

Nonpublic Institutional Data means any data created, owned, or processed by the university that is not publicly published or available.

Personal Information means any data or information that relates to, is associated with, describes, identifies, or reasonably can be used to identify a natural person.

Processing Data means the access, collection, classification, use, modification, sharing, storage, or destruction of data.

Processing Nonpublic Institutional Data

University employees may process Nonpublic Institutional Data only when doing so reasonably serves the university's academic, administrative, or institutional purposes.

University employees must process Nonpublic Institutional Data in accordance with applicable university policies, the BYU Privacy Notice, and relevant laws and regulations.

Accessing Nonpublic Institutional Data

The university allows access to Nonpublic Institutional Data only in accordance with the following table:

Accessing Individual or Party	Accessible Data
An individual (e.g., student, alum, employee, donor, patient, patron)	The individual's own Personal Information, subject to applicable laws and relevant BYU policies and procedures.

A university employee	Nonpublic Institutional Data as necessary for legitimate university purposes associated with his or her job, provided that the employee uses authorized university systems and processes, including approval by the assigned Data Stewards to ensure (i) appropriate use of the data to support university purposes, (ii) the confidentiality and privacy of those individuals whose records may be accessed, and (iii) compliance with applicable laws or policies with respect to access, use, and disclosure of the data.
A third party (e.g., consultant, contractor, vendor, CES school, Church department)	Nonpublic Institutional Data when the third party's access and use of the data is (i) for legitimate university purposes, (ii) approved by the assigned Data Stewards, and (iii) subject to a Data Sharing Agreement between the third party and BYU requiring the third party to take measures to appropriately safeguard and use the information pursuant to BYU policy and applicable laws.
Legal authorities, government agencies, or parties engaged in or preparing for legal proceedings*	Nonpublic Institutional Data, only if authorized by the Office of General Counsel.

*Any employee who, on behalf of the university, receives a request, subpoena, warrant, or court order for Nonpublic Institutional Data from one of these entities or individuals immediately must refer that request, subpoena, warrant, or court order to the Office of General Counsel.

Processing Personal Information

University employees must process Personal Information

- *purposefully*—in compliance with pre-defined and legitimate purposes, such as performing a contract, pursuing a legitimate interest, complying with law, or based on consent;

- *minimally*—in a manner that is sufficient to properly fulfill the stated purpose, has a rational link to that purpose, is limited to what is necessary, and for no longer than necessary;
- *transparently*—only after providing individuals with clear and intelligible information, either through concise privacy notices or just-in-time statements, about who will process their Personal Information and for what purposes, and by giving individuals the opportunity to inspect and correct their Personal Information as required by law; and
- *safely*—subject to appropriate measures, including role-based access controls, data sharing agreements, and other controls to safeguard against anticipated risks, where applicable.

Transferring Nonpublic Institutional Data

University employees should contact the Office of General Counsel (OGC) and the CES Security Operations Center (CES SOC) before signing any agreement or entering into any arrangement with a third party to process or have access to any Nonpublic Institutional Data. The CES SOC provides an assessment of the proposed data transfer(s) and the third party's security standards and mechanisms. (*See* Vendor Security Risk Assessment Process.) The OGC provides legal review of the information security and data transfer terms and conditions. (*See* Legal Documents Policy.)

Reporting Data-Related Issues

See the Reporting section of the Appropriate Use of Information Technology Resources Policy.

APPROVED: 27 Dec 2023 [Revised 6 Jan 2025]

PRIOR VERSION: 1 Mar 2021

APPLICABILITY: This policy applies to all members of the university community, visitors, affiliates, and business associates including students, faculty, staff, lecturers, instructors, third-party vendors, and any others with access to university information and all persons, systems, and activities where Nonpublic Institutional Data is stored, processed, or transmitted in either electronic or printed form.

POLICY OWNER: Information Technology Vice President and CIO

RESPONSIBLE OFFICE: Office of the Chief Information Security Officer, Office of the Chief Privacy Officer

IMPLEMENTING PROCEDURES:

- BYU Information Security Major Incident Response
- BYU OIT and CES SOC Data Requests
- BYU Student Health Center Privacy Practices
- Data Security
- Information Privacy Standard

RESOURCES:

- BYU Data Stewards
- BYU Info Hub
- BYU Information Security and Privacy
- BYU Privacy Notice

RELATED POLICIES:

- Access to Student Records Policy
- Appropriate Use of Information Technology Resources Policy
- Human Research Protection Policy
- Information and Records Retention Policy
- Merchant Credit Card / E-Commerce Policy
- Surveys Policy
- University Archives Policy