POLICY TITLE	Privacy and Disclosure	**Policy Number**	446
Section	Facilities, Operations, and Information Technology	**Approval Date**	May 9, 2023
Subsection	Information Technology	**Effective Date**	May 9, 2023
Responsible Office	Office of the Vice President of Digital Transformation	**Last Review**	May 9, 2023

1.0 PURPOSE

1.1 Utah Valley University (UVU) respects the privacy of its students, faculty, and staff and is committed to protecting the privacy of information within its control in a manner consistent with applicable laws, regulations, and university policies.

1.2 To provide services to students and employees, administer its programs, and perform contractual obligations, the University may collect, process, and transfer various types of personal data, including but not limited to names; application information; attendance; academic records; employment records; contact information including phone numbers, email addresses, and mailing addresses; and date of birth.

2.0 REFERENCES

2.1 *The Privacy Act of 1974*, 5 U.S.C. § 552a (1974)

2.2 *The Freedom of Information Act,* 5 U.S.C. § 552 (1977) (as amended by Pub. L. No. 104–231, 110 Stat. 3048)

2.3 *The Gramm-Leach-Bliley Act*, 15 U.S.C. § 6801 (1999)

2.4 *Family Educational Rights and Privacy Act (FERPA)*, 20 U.S.C. § 1232g (1974)

2.5 *Privacy of Consumer Information*, 16 C.F.R. § 313.1 (2000)

2.6 *Standards for Safeguarding Customer Information*, 16 C.F.R. § 314.1 (2021)

2.7 *Health Information Technology for Economic and Clinical Health Act (HITECH)*, Pub. L. No. 111–115 § 13001, 123 stat. 226 (2009)

2.8 *Health Insurance Portability and Accountability Act (HIPAA)*, Utah Code Ann. § 63-2-101 to -901 (1996)

2.9 *Government Records Access and Management Act (GRAMA)*, Utah Code Ann. § 63G-2-101 (2008)

2.10 *Electronic Information and Data Privacy Act*, Utah Code Ann. § 77-23c-101 et seq. (2019)

2.11 Utah Board of Higher Education Policy R840 *Institutional Business Communications*

2.12 UVU Policy 133 *Compliance with Government Records Access and Management Act*

2.13 UVU Policy 135 *Use of Copyrighted Materials*

2.14 UVU Policy 445 *Institutional Data Management and Access*

2.15 UVU Policy 541 *Student Code of Conduct*

2.16 UVU Policy 542 *FERPA (Student Records Act)*

3.0 DEFINITIONS

3.1 Confidential information: Any information that is not generally available to the public and that university has identified as confidential, that should reasonably be understood to be confidential, or that university is obligated to keep confidential under applicable laws, regulations, contractual obligations, university policies, or the policies of relevant government agencies, including but not limited to PII, student records, financial information, research data, and sensitive information.

3.2 Disclosure: The release, transfer, provision of access to, or other communication of information outside of the UVU community.

3.3 Personally Identifiable Information (PII): Unique identifiers, including a person's Social Security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone numbers, and personal email addresses.

3.4 Sensitive information: Race or ethnic origin, religion, political affiliations, sexual orientation, criminal history, and trade union or association memberships are all considered sensitive information. Any information about biometrics, genetics or medical history is also treated as sensitive information.

3.5 University community: University community members include all persons employed by or affiliated with Utah Valley University in any way and all persons participating in any university program or activity, including but not limited to trustees, advisory board members,

administrators, faculty, staff, students, independent contractors, volunteers, and guests or visitors to any university campus or any property owned or leased by the University.

3.6 UVU electronic communication systems: UVU-authorized and licensed systems for university-related communications, including communications by email, instant messaging, social media, file-sharing, websites, and other cloud-based offerings.

3.7 Institutional data: All UVU public, restricted, and sensitive data, whether in electronic or paper format, as defined in UVU Policy 445 *Institutional Data Management and Access*.

4.0 POLICY

4.1 Responsibilities of the University

4.1.1 UVU respects and values the privacy of its faculty, students, staff, and other constituents.

4.1.2 UVU limits the collection, use, disclosure, and storage of information that reasonably serves the University's academic, research, or administrative functions or other legally required purposes. Such collection, use, disclosure, and storage shall comply with applicable federal and state laws, regulations, and university policies.

4.2 Institutional Data as UVU Property and Records

4.2.1 All institutional data, including communications created for UVU business or maintained in technology assets or information systems, is the property of UVU in accordance with Policy 136 *Intellectual Property*. Institutional data, including those personal in nature and unrelated to university business, may be subject to public records requests under state law. Employees, including student employees acting in their capacity as employees, shall have no expectation of privacy when using university information systems, including but not limited to UVU networks, electronic communications systems, and other systems to store or transmit files, data, and messages, regardless of whether such systems are accessed on university-owned technology assets or an employee's own personal equipment.

4.2.2 The University does not routinely monitor individual usage of its electronic communication systems; however, consistent with this policy, institutional data that is transmitted over or stored in university electronic communication systems is subject to being monitored, reviewed, and disclosed to fulfill legitimate university business interests which may include, but are not limited to, the following:

4.2.2.1 To comply with legal requirements or process (e.g., Utah Governmental Records Access & Management Act or subpoena);

4.2.2.2 To yield information necessary for the investigation of a suspected violation of law, university policy, or any other applicable regulation or university policy governing disciplinary action;

4.2.2.3 To maintain the security of university computing systems and networks; for system administrators to diagnose and correct problems with system software or hardware; to yield information needed to deal with an emergency;

4.2.2.4 For the ordinary business of the university to proceed, (e.g., access to data associated with an employee who has been terminated/separated or is pending termination/separation, is deceased, is on extended sick leave, or is otherwise unavailable);

4.2.2.5 To comply with a written request on behalf of the parents, guardian, or personal representative of the estate of a deceased student; or

4.2.2.6 For research authorized by the university under a data use agreement that precludes the disclosure of personally identifiable information."

4.2.3 Notice of monitoring, reviewing, and disclosing will be provided when required by other university policies, such as those addressing misconduct.

4.2.4 Access to institutional data is a privilege that UVU may restrict wholly or partially without prior notice and without the employee's consent. Generally, access will be restricted only when there is reason to believe that serious violations of law or UVU policy have occurred, when an employee is placed on administrative leave, whether paid or unpaid, employment is terminated for cause, or when other urgent or compelling circumstances arise.

4.2.5 Employees shall not use institutional data or technology assets, including electronic communication systems for activities prohibited by law or UVU policy, for personal political activity or for activities that interfere with UVU operations.

4.2.6 Consistent with USHE Policy R840, employees or other designated individuals who conduct university business shall use only UVU electronic communication systems for university-related communications. Conducting university business on any personal or non-UVU enterprise email, unapproved electronic messaging or file-sharing systems, or other non-UVU electronic communication systems or methods is prohibited.

4.3 Unauthorized Access and Disclosure

4.3.1 Employees shall not attempt to gain unconsented access to another employee's university information or UVU electronic communication accounts where they lack a university business justification properly related to their job function.

4.3.2 2 Employees shall not disclose confidential information to unauthorized individuals or entities, including employees or third parties.

4.4 Mass Communications

4.4.1 Only departments authorized by University Marketing and Communications may send messages to the entire faculty, staff, administration, and/or student body using authorized methods.

4.4.2 Those who wish to send unsolicited messages to an external audience must seek preauthorization from their college/school/division University Marketing and Communications director or manager. (List of University Marking and Communications directors and managers can be found at https://www.uvu.edu/marketing/index.html.)

4.5 Photography and Recording on Campus

4.5.1 The University campus is public property. UVU community members may make photographs and videos, audio, and other recordings in university spaces that are generally open to members of the public, such as outdoor spaces and main hallways, in accordance with university policy.

4.5.2 Recording in classrooms, libraries, laboratories, gymnasiums, or other nonpublic spaces may occur only without disruption or distraction from the intended use and purpose of the space, as determined by the instructor or other authorized university manager of the space, and in accordance with university policy. Requests for photography or recording in nonpublic spaces should be directed to the Communications Office in University Marketing and Communications, who will coordinate with the relevant university managers.

4.5.3 Filming and photography may not use the University's name or trademarks in a way that infringes on those marks or that implies University endorsement for any product, service, or activity (see UVU Policy 136 *Intellectual Property*).

4.5.4 Photography or recording activities that substantially disrupt university activities, endanger people or property, or otherwise violate law or UVU policy are prohibited.

4.6 Responsibilities of University Privacy Officer

4.6.1 The University shall have a privacy officer who is appointed by the Vice President of Digital Transformation and who is responsible for the following:

1) Interpreting this policy; or

2) In conjunction with the Office of General Counsel, coordinating compliance with all privacy laws and regulations (except those specifically noted section 4.5 through 4.8); or

3) Improving privacy practices, promoting privacy best practices, and recommending privacy policies and policy changes in all areas related to privacy at UVU.

4.6.2 The university privacy officer will collaborate with UVU's information security officer, General Counsel, and other university privacy officials and university administration as appropriate.

4.7 FERPA Privacy Responsibilities

4.7.1.1 The university registrar has primary responsibility for establishing policies, procedures, and guidelines related to compliance with the *Family Educational Rights and Privacy Act (FERPA).* For more information, see UVU Policy 542 *FERPA (Student Records Act)*.

4.8 GRAMA Privacy Responsibilities

4.8.1 The university GRAMA officer has primary responsibility for establishing policies, procedures, and guidelines related to compliance with the *Government Records Access and Management Act.*

4.9 Responsibilities of System Owners

4.9.1 Each system owner and each individual who retains custody of information is responsible for complying with all related university policies for information under their care or control.

4.10 Legal and University Process

4.10.1 Notwithstanding section 4.1, for the proper functioning of the University and to protect the safety and well-being of individuals or the community, the University may disclose information in the course of investigations and lawsuits, in response to subpoenas, and as permitted by law.

4.10.2 To comply with privacy laws, UVU shall post its privacy statement on all websites collecting personal information.

4.11 Violations of This Policy

4.11.1 Any violation of this policy, including failure to follow proper university policies and procedures concerning access, storage, and transmission of information may result in disciplinary action up to and including termination of employment.

4.11.2 Members of the UVU community who believe that university policy has been violated should report such violations to the university privacy officer or Internal Audit. Complaints or concerns may also be reported anonymously by calling or reporting through the Report Concerns webpage at https://www.uvu.edu/audit/concerns/.

4.11.3 Any university unit found to have violated this policy may be held accountable for the financial penalties and remediation costs that directly result from this failure.

5.0 PROCEDURES

5.1 Required Privacy Notices Regarding Personally Identifiable Information

5.1.1 When UVU (or an authorized third party) collects personally identifiable information on one of the commercial areas of its website or as the operator of an online service, it will conspicuously post either a privacy policy or a link to a privacy policy on the portal page for the commercial activity. This policy will

1) Identify the categories of personally identifiable information collected through the commercial portions of the operator's website or through the operator's online service; and

2) Identify the categories of third parties with whom UVU may share that personally identifiable information; and

3) Provide a description of how an individual may request changes to their personally identifiable information collected through the website or online service and retained by UVU, if any process exists; and

4) Describe the process by which UVU will notify users of the commercial portion of UVU's website or its online service of material changes to UVU's privacy policy for that portion of the website or online service. It is sufficient to say that the policy will be updated online; and

5) Identify the effective date of the privacy policy and all updates.

5.2 UVU's General Data Protection Regulation (GDPR) Privacy Notice will be kept up to date and made available via a link at https://www.uvu.edu/legal/gdpr.html.

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity
May 9, 2023	New policy approved.	UVU Board of Trustees
September 22, 2026	Non-substantive change: Replace "EthicsPoint" with "Report Concerns"	UVU Policy Office