POLICY

Authority: P.L.106-102, RCW 19.215.020, RCW 40
45CFR164; RCW 42.56; RCW 9.73; 20 U.S. 1232; RCW 42.56

Effective Date: 
Approved by: 

See Also: 
POL-U6500.01 Filming, Photography or Video Production on University Property
POL-U3000.02 Using Electronic Methods for University Communication
POL-U6500.02 Using Social Media

POL-U5315.02 PROTECTING PERSONAL INFORMATION

This policy pertains to the appropriate collection, use, disclosure, and destruction of personal, personally identifiable, confidential, and protected information of individuals, including, but not limited to, students, employees, third-party vendors, visitors, that is collected, accessed, maintained, used, or disclosed by or on behalf of the University in any format.

See also the University’s policy on Securing Information Systems (POL-U3000.07)

Definitions:

Personal Information:

- Information about an individual, including but not limited to, first name or first initial and last name in combination with social security number, license or state ID number, date of birth, private (encryption) key, student, military, or passport identification number, health insurance policy number or health insurance identification number, medical history or mental or physical condition, medical diagnosis or treatment, biometric data (fingerprints, voice, etc.), and username or email in combination with password (RCW 19.255), and

- When an individual is covered by the General Data Protection Regulation (GDPR), any information relating to their identified or identifiable natural person when within the territorial scope of the GDPR.

Privacy: A reasonable expectation to be free from unwanted or undue intrusion in one’s private life, affairs, or data and the right for individuals to control their own data and to specify how and when that data is collected, used, monitored, shared/disclosed, and/or destroyed, within the limits of the law.

Protected Data: Data that falls into one of the three following data classifications:
POLICY

- Sensitive Information: Information that may not be specifically protected from disclosure by law but is for official use only.

- Confidential Information: Information that is specifically protected by applicable state, federal, or international law from unauthorized disclosure such as but not limited to Personal Information, non-public financial information, and employee personnel records.

- Confidential Information Requiring Special Handling: Information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated, such as by statutes, regulations, or agreements, or that serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions. Examples include physical and mental health records, substance abuse treatment records, educational records, tax returns, and some criminal justice information.

1. Western Washington University is Committed to Protecting Personal Information

Western Washington University is committed to appropriate use, collection, monitoring, disclosure, and destruction of an individual’s Personal Information and Protected Data within its control in a manner consistent with applicable laws, regulations, University policies, and Western’s strategic mission and values.

2. Western to Maintain a University Privacy Program

Following the effective date of this policy, the University will establish and maintain a centralized Privacy program ("Program"). Through the Program, privacy compliance owners and strategic partners will strive to balance business operational needs with individual privacy rights in a cohesive, comprehensive, and proactive manner based on established principles. The Program principles will reflect, at a minimum, the Fair Information Practice Principles established by the Federal Trade Commission:

a) **Notice/awareness:** Individuals are given notice of the institution’s information practices and the purposes for data collection before any personal information is collected in order to make an informed choice about participating in the data collection.

b) **Choice/consent:** Individuals are given options to control how their data is used including secondary uses of that information based on disclosing the purpose of the collection. The notion of consent extends beyond the stated purpose for which the information was originally collected, and individuals can withdraw their consent at any time.

c) **Access:** Individuals are given the ability to view the data collected. The access is to be timely and inexpensive.
4) **Integrity/security:** Information collectors properly secure the collected data from unauthorized access or disclosures and honor requests to correct personal data if inaccurate or incomplete.

5) **Enforcement/Redress:** Individuals are given the means to report suspected violations. Compliance is enforced and necessary corrective action is taken by the institution.

3. **Privacy Program to be Transparent**

The Program must be detailed and published to include, at a minimum,

a) A Privacy Compliance Committee and charter,

b) A reporting structure for effective leadership oversight,

c) Identification of privacy compliance owners and their roles and responsibilities,

d) An action plan that addresses the federally required elements of an effective compliance program which includes a risk assessment, policy development, training, monitoring, and reporting activities (see University Compliance Program document), and

  e) Contact information for individuals to exercise their rights.

4. **University Privacy Program Supplements University Information Security Program**

The University’s Privacy Program is partially dependent on the University’s Information Security Program which promotes a secure environment for protecting the integrity, confidentiality, and availability of University data, including Personal Information and Protected Data.

The Privacy Program is to establish a coordinated effort with the Information Security Program in meeting the University’s compliance requirements and ethical responsibilities as they pertain to an individual’s Personal Information and Protected Data.

5. **Privacy Compliance Owners Responsible for Overseeing Compliance**

Delegated privacy compliance owners (see Compliance Matrix – Information Category) are responsible for overseeing compliance in their respective privacy areas including the development of and training on policy, standards, and procedures imperative for cultivating a workplace culture and governing University operations in a manner consistent with privacy regulations and the mission of the Program. See also University Compliance Program – Roles and Responsibilities.
The Program will ensure the integration of the multitude of privacy regulations within the policy development process to more effectively and efficiently communicate expectations to employees.

The University Compliance Manager is delegated as the University Privacy Coordinator responsible for facilitating the development and publication of the Program and reporting on progress to leadership.

6. **All Employees are Responsible for Appropriate Handling of Personal Information and Protected Data**

All University employees must maintain the highest level of integrity and responsibility in collecting, protecting, using, disclosing, and destroying individuals’ Personal Information or Protected Data to which they may intentionally or accidentally gain access.

Regardless of their access permissions or role with the University, employees must strictly adhere to all written Privacy and information security related policies, standards and procedures and use professional judgement in the absence of written guidance. Any questions regarding the handling of privacy or information security issues should be addressed to the appropriate compliance owner. See also *Securing Information Systems Policy* (POL-U3000.07)

All faculty and staff will be required upon hire, and then annually, to sign a confidentiality statement agreeing to adhere to the requirements of this policy and related standards and procedures. Failure to sign such a statement in no way diminishes the individual’s obligation to uphold Western’s policies.

7. **Expectation of Privacy is Limited**

Access to Personal Information or Protected Data maintained by or is accessible to the University will be granted based on an individual’s University position duties and business need. All Personal Information or Protected Data access procedures and decisions are to be based on the “minimal necessary only” principle.

Western respects and values the privacy of its faculty, students and staff and will not monitor its community members without cause except as permitted or required by law, policy, and/or agreements (including University Residences agreements) and in accordance with written policy, standards, and/or procedures. See also *Using Electronic Methods for University Communication Policy* (POL-U3000.02)

The University may access and/or disclose an individual’s information without their consent as permitted or required by law, or for due cause and in accordance with University written policy, standards, and/or procedures.
When access or disclosure is permissible but not required, the University will first consider the rights and the interests of the individual and follow relevant access and/or disclosure standards and procedures.

8. **Public Records Requests Comply with Exemption Rules**

Only records subject to public disclosure laws will be released upon request in accordance with University procedures. All record requests are reviewed for legal exemptions prior to being released. The University Public Records Officer oversees public records program in accordance with state law (RCW 42.56).

9. **Management Responsible for Enforcement**

Supervisor at all levels are responsible for understanding and enforcing privacy and information security policies, standards, and procedures.

10. **All Employees Responsible for Reporting Known or Suspected Violations**

Employees must promptly report known or suspected privacy violations in accordance to written procedures.