Information Privacy

UNIVERSITY POLICY #082

Authority: BOG Rule 60: Information Technology Governance
Approval Date: October 6, 2021
Effective Date: October 6, 2021
Revision History: None
President's Signature: On File

SECTION 1: Purpose and Scope

1.1 The purpose of this Policy is to establish the rules that govern the University safeguards regarding the privacy of students, employees, University business, and other matters by protecting records maintained in any type of physical or Electronic Record classified as Confidential Information.

1.2 This Policy applies to all University Faculty, Staff, Students, visitors, and third parties who are doing work on behalf of the University.

SECTION 2: Principles

2.1 **Notification.** Users should be notified that information is being collected and they should be informed of their rights (e.g., all Web pages that collect personally identifiable information should include a privacy notice that specifies how the information will be used).

2.2 **Minimization.** The University should gather as little information as possible for legitimate purposes and delete information when it is no longer needed or no longer required by law to be retained (e.g., library records need not be kept for more than a certain limited period of time).

2.3 **Secondary User Information.** Users should only use individual information for the purposes for which it was collected unless the individual gives additional consent (e.g., a department should not share information with an administrative office for a separate purpose without the individual's knowledge and consent).

2.4 **Nondisclosure and Consent.** Information should not be released to third parties external to the University without consent (e.g., vendors, business, etc.).

2.5 **Need to Know.** Only those with legitimate, official needs should have access to information (e.g., a person's position of authority in the University does not necessarily mean that they should be able to access information).

2.6 **Data Accuracy, Inspection, and Review.** Personal Information must be accurate, and individuals should have the right to examine information about themselves and request changes (e.g., employees should be able to review their records and make changes or follow a standard process for any information that is disputed).

2.7 **Information Security, Integrity, and Accountability.** Information should be secure and not vulnerable to unauthorized modification, and the handling of the data must be subject to accountability (e.g., it should always be known who has access to information and changes to information should be documented).

2.8 **Education.** The University has the responsibility to educate its constituents concerning privacy rights and the proper handling of information (e.g., all constituents should know whom to consult about these matters and all employees should understand their responsibilities for abiding by policies for information handling).

SECTION 3: Record Classification

3.1 The President and/or his/her designee(s) will appoint a group of "Data Stewards" who will, in consultation with legal counsel and the West Virginia Higher Education Policy Commission, determine the confidentiality of the data. They are responsible for developing procedures for creating, maintaining, and using University data, based on University policy and applicable state and federal laws.

3.2 The classification Confidential Information covers sensitive information about individuals, including information identified, in accordance with West Liberty University policy and procedure, and sensitive information about the University. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include information about:

3.2.1 Current and former students (protected under the Family Educational Rights and Privacy Act (FERPA) of 1974), including student academic, disciplinary, and financial records and student works such as homework, term papers, and exams; and prospective students, including information submitted by student applicants to the University.

3.2.2 Current, former, and prospective employees, including employment, pay, health, and insurance data, and other personnel information.

3.2.3 Research, including information related to a forthcoming or pending patent application and information related to human subjects.

3.2.4 Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.

3.2.5 Information security data, including passwords.

3.3 **Determining Authorizations.** Only those with legitimate, official need have the access to these classified Electronic Records. Data Stewards determine who is authorized to have

access to their information. They should make sure that those with access have a need to know the information and know the security requirements for that information. For Confidential Information, they should also make sure that those given access have a need to know and have signed a confidentiality agreement that covers the information.

3.4 **Data Breach.** Should a Data Breach or potential breach be suspected, individuals should report the incident to the University Privacy Officer within 48 hours. The Privacy Officer will follow the steps required in the Data Breach Response Policy (University Policy 081).

SECTION 4: Enforcement and Interpretation

4.1 Any employee who violates this Policy will be subject to appropriate disciplinary action.

4.2 Any student who violates this Policy will be subject to appropriate disciplinary action in accordance with the Student Code of Conduct.

4.3 Any individual affiliated with the University who violates this Policy will be subject to appropriate corrective action, including, but not limited to, termination of the individual's relationship with the University.

4.4 The University's Information Technology Director/Privacy Officer will coordinate with appropriate University entities on the implementation and enforcement of this Policy.

4.5 Responsibility for interpretation of this Policy rests with the President and Information Technology Director/Privacy Officer.

SECTION 5: Definitions

5.1 **"Authorized Individuals"** means faculty, adjuncts, staff, students, authorized visitors, guests, and others who have assigned WLU Login credentials which provides them access to University IT Resources.

5.2 **"Electronic Record"** means a form of an electronic record, whether or not any of the electronic communications resources utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print the electronic communications record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature as a University electronic record for purposes of this or other University policy. Until determined otherwise or unless it is clear from the context, any electronic record residing on university-owned or controlled telecommunications, video, audio, and computing facilities will be deemed to be a University electronic record for purposes of this Policy.

5.3 **"Data Breach"** means the unauthorized access and acquisition of unencrypted and unredacted computerized data or physical records that compromise the security or confidentiality of personal information maintained by the West Liberty University.