ITS Policy 3.0
Information Privacy Policy

Category: Information Technology
Information Privacy
Title: Information Privacy Policy
Responsible Unit: Information Technology Services
Effective: August 1, 2018
Revision History: Originally adopted March 16, 2017
Review Date: August 2021

INFORMATION TECHNOLOGY SERVICES POLICY 3.0
INFORMATION PRIVACY POLICY

1. PURPOSE & SCOPE:

1.1 ***Purpose***. West Virginia University (University) respects the privacy of an individual and seeks to limit the collection, access, use, disclosure, and storage of personal data. The purpose of this Policy is to:

1.1.1 Identify the personal data the University collects;

1.1.2 Identify how the University collects personal data; and,

1.1.3 Explain how the University uses and protects the personal data it collects.

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

2. INFORMATION PRIVACY AT THE UNIVERSITY:

2.1 The University seeks to limit the collection of personal data to that which reasonably serves its academic, research, outreach, and administrative functions.

2.2 The University collects personal data through websites and social media pages, that does not reveal specific identities, including but not limited to: geographic location, device, internet browser, and operating system.

2.3 The University will not collect personally identifiable data (PII), such as name, address, Social Security number, or financial information, without an individual's expressed consent. The University collects PII through:

2.3.1 Applications made available for use on or through computers and mobile devices;

2.3.2 HTML-formatted email messages sent by the University;

2.3.3 Patient care, health treatment, and research;

2.3.4 Offline activities (e.g., campus visit, attend seminar, place a request over the phone); and,

2.3.5 Other sources such as publicly available databases or joint marketing partners who share information with the University.

2.4 The University uses PII for legitimate business and operational purposes including, but not limited to:

2.4.1 Provide services, complete transactions, fulfill requests, and send administrative information;

2.4.2 Provide newsletters and/or other promotional materials;

2.4.3 Analyze, aggregate, and anonymize data for reporting.

2.5 The University will not sell, market, or otherwise distribute PII without authorization, except when necessary to provide a service or to support its mission. The University may disclose PII:

2.5.1 To affiliates or third-party service providers with whom it has a contractual agreement;

2.5.2 To facilitate business operations within the University;

2.5.3 To protect the safety and well-being of individuals or the community; and,

2.5.4 As permitted or required by law.

2.6 When the distribution of PII is necessary, the distribution will be subject to reasonable terms and conditions that, among other things:

2.6.1 Limit the access to and use of the data to only authorized individuals for legitimate business purposes;

2.6.2 Ensure the data will remain secure; and,

2.6.3 Ensure the data will be returned or destroyed when its purpose for distribution ends.

2.7 The University will implement safeguards to secure the integrity and confidentiality of PII collected including, but not limited to:

2.7.1 Publishing associated standards and procedures identifying the minimum requirements to safeguard PII.

2.7.2 Educating and providing awareness to its workforce regarding safeguarding PII.

2.8 Unauthorized access or disclosure of PII must be reported to Information Technology Services within 24 hours of the event as per the Information Security Event Response Policy.

2.9 The University may disclose PII deemed Directory Information at its discretion.

2.10 The University will retain PII according to the Record Retention Policy and Schedule.

2.10.1 All personal data will be destroyed in accordance with best practices and as required by applicable laws at the time of destruction.

2.11 The University will ensure that data processed or stored in University systems hosted by third-party vendors are compliant with this Policy and relevant laws and regulations; however, the University is not responsible for the information collection, use, disclosure, or security policies or practices of third-party service providers.

2.12 All University units are responsible for establishing and making available for view appropriate privacy notices related to their collection, use, distribution, and destruction of personal data.

2.13 Those University units designated as a University health care component may use and share personal health information (PHI) across locations to facilitate treatment, research, payment, and other healthcare operation purposes.

2.14 Individuals have the right to:

2.14.1 Expect that their PII collected by the University will remain private and secure;

2.14.2 Access and review their PII to confirm accuracy and completeness;

2.14.3 Be notified when PII has been disclosed or accessed by an unauthorized person;

2.14.4 Request to amend or delete their PII, if appropriate;

2.14.5 Opt out of receiving electronic communications; and,

2.14.6 Request the University withhold disclosure of their PII.

2.15 Individuals are advised to be discreet and cautious in their use of University technology resources and are obliged to abide by the Acceptable Use of Data and Technology Policy.

2.16 Individuals who disclose other people's personal information to the University or our third-party service providers, represent that they have the authority to do so and permit us to use the information in accordance with this Policy.

2.17 PII collected by the University must not be misused. Misuse includes, but is not limited to the following:

2.17.1 Seeking or soliciting Social Security numbers via email or phone;

2.17.2 Sending or knowingly accepting credit card information by email;

2.17.3 Storing credit card information on University-owned computers;

2.17.4 Unnecessarily accessing PII;

2.17.5 Using PII of another person for personal gain;

2.17.6 Not reporting when PII is stored inappropriately or disclosed;

2.17.7 Unilaterally updating PII without the individual's request or consent; and,

2.17.8 Compiling copies or duplicates of PII without the individual's approval, except for back up or disaster recovery purposes.

2.18 Misuse of personal data is a violation of this Policy.

2.18.1 Any Faculty or Staff who violates this Policy shall be subject to appropriate disciplinary action.

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

2.18.3 Any individual affiliated with the University who violates this Policy shall be subject to appropriate corrective action, including, but not limited to, cancellation of their relationship with the University.

2.19 The University will never take retaliatory action against a Student, Patient, Physician, Employee, or any other person for exercising their rights established under this Policy, including submitting a complaint or reporting a violation.

2.19.1 Any attempt to retaliate against a person for reporting a privacy violation may itself be considered a violation of this Policy and may result in sanctions.

2.20 The University reserves the right to update this Policy at any time in the future.

2.20.1 The University also reserves the right to make the revised change notice effective for personal data already collected or will receive in the future.

---

3. DEFINITIONS:

3.1 **Confidentiality**: A set of rules that limit access or place restrictions on certain types of information to protect personal privacy and proprietary information.

3.2 **Directory information**: The University considers the following information it collects Directory Information: name, official address, telephone number, place of birth, age of student, names and addresses of parents, major and minor fields of study, class status (e.g., freshman), enrollment status (e.g., full-time, part-time), dates of attendance, previous educational institution(s) attended, degree(s) and date(s) conferred including anticipated graduation dates, awards, honors, participation in officially recognized sports and

activities, physical factors of athletes, and duties, responsibilities, and dates of service of Graduate Assistant, Student Workers, Interns, or Student Volunteers.

3.3 **Integrity:** The overall completeness, accuracy, and consistency of the data.

3.4 **Personal data:** Data associated with an individual person.

3.4.1 ***Other personal information***: Data that does not identify a specific identity or relate to an identifiable individual unless combined with other personal data such as physical location, IP address, browser/device information, app usage data, demographic information, appearance, religion, political opinions, and behavior.

3.4.2 ***Personally identifiable information (PII)***: Data that specifically identifies an individual, including, but not limited to: Social Security number, driver's license number, credit card numbers, bank account information, protected health information (PHI), employee performance or salary information, student grades, disciplinary information, or account passwords.

3.4.3 ***Protected Health Information (PHI):*** Data that identifies health status, provision of health care, or payment for health care that is created or collected and can be linked to a specific individual.

3.5 **Third-party services:** An individual or an entity that has a contract, license, or other arrangement with the University to provide a technology service.

3.6 **University information systems:** The hardware, software, and related technology that supports the academic, administrative, learning and research operations at the University.

4. ENFORCEMENT & INTERPRETATION:

4.1 WVU's Chief Information Officer, supported by the Chief Information Security and Privacy Officer, will coordinate with appropriate University entities on the implementation and enforcement of this Policy and other privacy policies.

4.2 Responsibility for interpretation of this Policy rests with the Chief Information Officer.

5. AUTHORITY

5.1 **Freedom of Information Act of 2000.**

5.2 **Privacy Act of 1974.** 5 U.S.C. § 552a.

5.3 **The Family Educational Rights and Privacy Act (FERPA)**, 20 U.S.C. § 1232g or 34 C.F.R Part 99.

5.4 **The Health Insurance Portability and Accountability Act of 1996 (HIPAA).** 45 C.F.R. § 160 and 164; 45 C.F.R. § 164.302 - § 164.318.

5.5 **General Data Protection Regulation (GDPR).** Regulation (EU) 2016/679.

5.6 **Gramm–Leach–Bliley Act (GLBA)**, also known as the Financial Services Modernization Act of 1999, Pub.L. 104–102 or 113 Stat. 1338. 15 U.S.C. § 6801-09; 16 C.F.R. § 313-314;

---

6. CROSS REFERENCES:

6.1 All other University policies are also applicable to the electronic environment. Relevant institutional policies include, but are not limited to:

6.1.1 ITS Acceptable Use of Data and Technology Resources Policy

6.1.2 ITS Information Security Event Response Policy

6.1.3 WVU Record Retention Policy & Schedule

6.1.4 Family Educational Rights and Privacy Act (FERPA)

6.1.5 WVU FERPA Policies

6.1.6 WVU HSC Notice of Privacy Practices

6.1.7 West Virginia Freedom of Information Act