The University of Vermont

OFFICE OF AUDIT AND COMPLIANCE SERVICES
UVM.EDU/POLICIES

POLICY

Title: Privacy

Policy Statement

The University of Vermont is committed to safeguarding the privacy of Non-Public Protected Data ("NPPD") that is collected, accessed, used, disclosed and/or stored by the University, as further defined herein. The University is also committed to compliance with the numerous laws that it is subjected to which govern the collection, access, use, disclosure and protection of NPPD. Compliance with these laws, regulations and corresponding University Policies and Procedures is required.

Reason for the Policy

This policy is intended to (i) reduce the risk of violations to the various laws, regulations and policies and procedures related to the safeguarding of NPPD; and (ii) minimize the risk of improper access, use and disclosure of the University's NPPD; and (ii) provide guidance on University expectations related to safeguarding of NPPD.

Applicability of the Policy

This Policy and accompanying UOPs apply to all members of the University community who access, use and/or disclose NPPD, including, without limitation, faculty, staff, students, contractors, consultants, temporary employees, and affiliates of the University.

Definitions

Data Subject: is a person whose information the University collects, processes, uses, accesses and/or discloses regardless of the format of the data (i.e., electronic, paper, recorded). See 'Identifiable Natural Person'. For the purpose of this policy, Data Subject also includes parents and legal guardians.

Identifiable Natural Person: is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Also known as 'Data Subject'.

Non-Public Protected Data (NPPD): is a UVM term and it includes, without limitation, personally identifiable information, protected health information, protected student information, and

protected library records as described below. NPPD includes data maintained in any electronic, recorded or hard copy format. NPPD includes all of the following:

- *Confidential Information:* is non-personal, non-public information that the University, a regulatory agency or another authority has determined must be kept private. This generally includes proprietary information, trade secrets, intellectual property, inventions and research data/results, user login credentials, technology systems and network information, information security plans and data mapping, and information that is otherwise exempt from the Vermont Open Records Law.

- *Controlled Unclassified Information (CUI):* is information that is provided by agencies of the federal government generally, but not exclusively, for research purposes. CUI requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

- *Non-Public Information (NPI)*: under the Gramm-Leach-Bliley Act (GLBA), non-public information is defined as any information that is not publicly available and that (i) a consumer provides to a financial institution to obtain a financial product or service from the institution; (ii) results from a transaction between the consumer and the institution involving a financial product or service; or (iii) a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

- *Personal Data (PD)*: under the European Union's General Data Protection Regulations (GDPR), personal data is defined as any information relating to an identified or identifiable natural person (Data Subject).

- *Personally Identifiable Information (PII)*: under 9 V.S.A. §2430(5)(A) is defined as an individual's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized person:
    - Social Security number;
    - a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;
    - a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;
    - a password or personal identification number, or other access code for a financial account;
    - unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
    - genetic information; and

- health records or records of a wellness program or similar program of health promotion or disease prevention, a health care professional's medical diagnosis or treatment of the consumer, or a health insurance policy number.

- *Protected Health Information (PHI)*: under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), PHI includes individually identifiable health information as defined at 45 CFR §160.103 that is transmitted or maintained by the University's covered HIPAA components; PHI also includes identifiable health information that is obtained by a University member pursuant to an agreement with another organization, such as a business associate agreement (BAA), or with a governmental entity and which is protected under the HIPAA/HITECH Act.

- *Protected Library Records*: under many state laws, including Vermont's 22 V.S.A. § 172, protected library records means (i) patron registration records that contain the information a University library patron must provide to be eligible for library privileges; and (ii) patron transaction records that contain personally identifiable information related to an individual's activities within the University libraries.

- *Protected Student Education Records*: means those records maintained by the University, whether by academic or administrative units, and protected under the Family Educational Rights and Privacy Act (FERPA) and as described more fully in the UVM FERPA Rights Disclosure policy.

Protected Personal Data (PPD): includes, without limitation, any NPPD relating to an identified or identifiable natural person. It includes NPI, PD, PII, PHI, PLR and PSER as defined above.

Public Information: describes information that may be legally disclosed to any person inside or outside the University. This information includes, but is not limited to, directory information and other information that the University makes accessible in its public documents, publications or website. In some cases, the University can only make this information public if it has notified the individual and given them the opportunity to object to the disclosure. Public information also includes information that the University may not make public or disclose as a matter of ordinary practice, but may be required to be disclosed upon receipt of a public records request.

Regulated Data: data that requires the University to implement specific privacy and security safeguards as mandated by federal, state, international, and/or local law, or University policy or agreement. Examples of regulations and categories include:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Social Security Numbers (SSNs)
- Gramm Leach Bliley Act (GLBA)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Sensitive Identifiable Human Subject Research
- Export Controlled Research - International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR)
- Library patron records protected under Vermont law (22 V.S.A. §§ 171-173)

Procedures

I. Public Records

The University is a public institution and subject to Vermont Open Records Act. Not all NPPD is protected by law. Some NPPD may be considered Public Information. In certain circumstances, this information may be shared by the University; however, all public records requests must comply with UVM's Records and Documents Requests Policy. Other members of the UVM community may not respond to any Open Records request without express permission from the University's Public Records Act Official.

II. Collection

The University will collect the minimum amount of NPPD that is necessary to conduct University business. If the NPPD is not necessary to satisfy a business-related purpose, it must not be collected.

Prior to collecting NPPD, the need must be assessed to determine the minimum amount of NPPD necessary to satisfy the purpose. NPPD can only be collected by lawful and fair means and members of the University community authorized to collect NPPD must be transparent regarding the planned and anticipated uses of NPPD. Where appropriate, Data Subjects must be advised the reasons for collection no later than the time of data collection and under certain conditions, consent must be obtained from the Data Subject prior to the collection and/or use of the NPPD.

III. Access and Use

The University will limit the access, use and disclosure of NPPD as prescribed by University Policies and Procedures and in accordance with applicable federal, state and international laws and regulations.

Access to NPPD will be assigned based on purpose of the access and role of the individual. Whenever possible, a technology solution will be implemented to control access. In the event that it is technologically infeasible to limit access, access will be limited based on policy. For more information on the appropriate use of assigned credentials, see the University Computer, Communication, and Network Technology Acceptable Use Policy.

Members of the University community with access to NPPD are prohibited from accessing this information outside the scope of their job duties. Given current technology and the varying level of security capabilities, there may be instances where an employee has the ability to access NPPD or confidential information that is outside the scope of their job duties. In these instances, employees are solely responsible to restrict access to that which is required to perform their jobs. Accessing NPPD outside the scope of their job may result in disciplinary action up to, and including, termination.

Once access has been authorized, members of the University community may only use that NPPD to perform official University business or to satisfy an official University need and only when granted permission to do so under University Policy, UOP or expressly by a manager or supervisor. Unauthorized or improper use of NPPD or confidential information creates significant risk to the University and, in some cases, may violate state, federal or international law for which the individual committing the violation may be held personally liable.

IV. Disclosure

The University will limit the disclosure of NPPD to that which is allowed and/or required under University Policies, Procedures, and under applicable federal, state and international laws and regulations. Members of the UVM community shall not share NPPD or confidential information either internally or

with third parties unless required to do so to transact University business, to comply with federal, state or international law or regulation, as required under University policies and disclosure statements/privacy notices, or when the data subject has been notified of the intended use and has freely given consent for this use. Members of the University community authorized to disclose NPPD will also ensure that the NPPD or confidential information only be disclosed to an authorized recipient.

V. Safeguarding/Data Security

The University's Information Security Policy and Procedures address safeguarding of NPPD, confidential information, and available technology designed to meet the University's regulatory requirements.

VI. Data Quality/Accuracy and Retention

NPPD maintained by the University should be relevant for the purpose for which they are being used. The information must be accurate, complete and kept up-to-date. It is the responsibility of the collector of the NPPD or confidential information to monitor it for accuracy on a periodic basis and that it is deleted when it has reached its useful life. Refer to the University's Records Retention Schedule for retention requirements. If the record is not listed, contact the Chief Privacy Officer for questions related to retention.

VII. Individual Rights

In addition to this policy, the University has issued other policies and/or statements addressing an individual's rights and protections concerning specific personal information. These include:

- the FERPA Rights Disclosure Policy for Student Educational Records;
- the HIPAA privacy notices for PHI obtained by the University's covered HIPAA components;
- the General Privacy Notice and Website Terms of Use for those University websites that collect personal information;
- the General Data Protection Regulation notices and consents for the collecting and processing of Protected Data related to European Union Data Subjects; and
- the University Libraries Confidentiality Policy Statement and Procedures for protected library records.

VIII. Third Parties

Agreements with third party vendors or consultants who will have access to NPPD must ensure that the vendor is subject to obligations of privacy, security and confidentiality that will enable the University to continue to comply with its own obligations under applicable laws and regulations. To reduce the likelihood that a contract or agreement will be delayed, those contemplating an agreement for information technology, digital or electronic products or services should consult with the Office of Information Security as soon as possible in the process; ideally prior to the contract phase.

IX. Statutory Exemptions

Laws protecting the privacy and confidentiality of information generally include exemptions to allow compliance with subpoenas, court orders, or other compulsory requests from law enforcement agencies. University Employees who receive such compulsory requests must follow the Subpoenas, Complaints, Warrants and other Legal Documents Policy.

X. Breach Notification

The University may have breach notification responsibility depending on the type of data that has been breached and the regulations impacting that data. Suspected breaches of NPPD must be reported in accordance with the University's Data Breach Notification Policy.

XI. Violations and Disciplinary Action

Individuals violating policies, procedures or regulations related to information privacy may face disciplinary action up to, and including, termination. Depending on the type and/or severity of the violation, the University may be required to file a report with applicable branches of the federal or state government, to international enforcement agencies or to law enforcement and, in those cases, individuals violating these regulations may be held personally liable for civil or criminal sanctions imposed as a result of the violation.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	**Contact Information:**
Chief Privacy Officer	privacy@uvm.edu
Chief Information Officer	cio@uvm.edu
Information Security Officer	ciso@uvm.edu
Dean of Libraries	bhref@uvm.edu
Registrar	registrar@uvm.edu

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- Code of Conduct and Ethical Standards
- Data Breach Notification
- FERPA Rights Disclosure
- HIPAA Disclosures
- Information Security
- Privacy Services – Additional Information on Privacy Issues
- Records and Documents Requests
- Records Management and Retention
- Subpoenas, Complaints, Warrants and other Legal Documents
- University of Vermont Libraries Confidentiality Policy Statement and Procedures

Regulatory References/Citations

- Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Genetic Information Nondiscrimination Act (GINA)
- Gramm-Leach Bliley Act (GLBA) (15 USC § 6801-6809)
- Health Information Technology for Economic and Clinical Health Act (HITECH) of HIPAA (45 CFR Parts 160 and 164)

- Health Insurance Portability and Affordability Act (HIPAA) (45 CFR Parts 160, 162 and 164)
- The European Union's General Data Protection Regulations (GDPR)
- Vermont Disclosure of Information Statute (18 V.S.A. § 7103)
- Vermont Library Patron Records Act (22 VSA 171 et. seq.)
- Vermont Protection of Personal Information (62 V.S.A. § 2430)
- Vermont Security Breach Notice Act (9 V.S.A. § 2435)

Training/Education

Training/education related to this policy is as follows:

Training Topic:	FERPA		
Training Audience:	Employees/Faculty with Access to Student Record Information	**Delivered By:**	Registrar's Office
Method of Delivery:	Self-Study	**Frequency:**	Upon Hire

Training Topic:	Gramm-Leach-Bliley Act (GLBA)		
Training Audience:	Employees/Faculty with Access to Student Financial Aid Information	**Delivered By:**	Student Financial Services (SFS)
Method of Delivery:	Self-Study	**Frequency:**	Prior to Granting Access and Annual Refresher

Training Topic:	Health Insurance Portability and Accountability Act (HIPAA) Training		
Training Audience:	Employees/Faculty in Covered Components with Access to PHI	**Delivered By:**	Covered Component Privacy Officer(s)
Method of Delivery:	In-Person	**Frequency:**	Prior to Granting Access and Annual Refresher

About this Policy

Responsible Official:	Chief Privacy Officer	**Approval Authority:**	President
Policy Number:	V. 9.2.4	**Effective Date:**	March 19, 2020
Revision History:	11/2011, 07/2012, 07/2014, 05/2015, 10/2016, 6/2020, 8/2020		