Personally Identifiable Information (PII)

Policy Effective Date: 3/24/2017 • **Policy Revised:** Insert
Procedures Effective Date: Insert • **Procedures Revised:** Insert

Policy Name: Personally Identifiable Information

Policy Purpose

This policy specifies how ETSU creates, collects, maintains, uses, and transmits Personally Identifiable Information (PII) relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and employees.

Applicability

This policy is applicable to all members of the ETSU community, including, but not limited to, students, alumni, employees, visitors, volunteers, third party vendors, and other agents or affiliates of the institution that are associated with the university or whose work gives them custodial responsibilities for PII.

Responsible Official, Office, and Interpretation

Information Technology Services is responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Data Custodians

Data Custodians are individuals responsible for oversight of PII in their respective areas of institutional operations.

Institutional ID

The Institutional ID, referred to as the ENumber, is a unique alphanumeric identifier assigned by the institution to any entity that requires an identifying number in an institution system or record.

Policy Name: Personally Identifiable Information

Personally Identifiable Information (PII)

(A) Means an individual's first name or first initial and last name, in combination with any one or more of the following data elements: (1) Social security number; (2) Driver license number, or (3) Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (B) Does not include information that is lawfully made available to the general public from federal state, or local government records or information that has been redacted, or otherwise made unusable.

Policy Name: Personally Identifiable Information

Policy

ETSU is committed to protecting PII against inappropriate access and to maximizing trust and integrity by implementing controls in compliance with applicable laws and regulations.

ETSU's Student Education Records Policy addresses student education records and confidential information with respect to currently and previously enrolled students; information related to FERPA can be found on the Office of the Registrar's website.

1. Requirements.

Members of the ETSU community will employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of PII, irrespective of its source, ownership, or the medium used to store it. All individuals who create, collect, maintain, use, and transmit PII have the responsibility to safeguard that information.

In adopting this policy, the University is guided by the following objectives:

1.1.1. Enhance individual privacy for members of the ETSU community through the secure handling of PII.

1.1.2. Ensure all members of the ETSU community understand their obligations and individual responsibilities under this policy.

1.1.3. Increase the security and management of social security numbers (SSNs) by:

1.1.3.1. Instilling broad awareness of the confidential nature of SSNs;

1.1.3.2. Establishing consistency with regard to appropriate use of SSNs throughout the university;

1.1.3.3. Ensuring that access to SSNs for the purpose of conducting ETSU business is granted only to the extent necessary to accomplish a given task or purpose; and

1.1.3.4. Reducing reliance on the SSN for identification purposes as much as possible.

1.1.4. Comply with all Payment Card Industry (PCI) standards.

1.1.5. Comply with any other applicable and required standards, regulations, and/or laws.

1.1.6. Comply with the Family Educational Rights and Privacy Act of 1974 (FERPA).

Data Custodians are responsible for oversight of PII in their respective areas of institutional operation. Activities of Data Custodians must align with this policy.

Officials responsible for each area, including but not limited to the below, shall be considered Data Custodians:

1.1.6.1. Student Records;

1.1.6.2. Financial Aid Records;

1.1.6.3. Alumni and Donor Records;

1.1.6.4. Employee Records;

1.1.6.5. Purchasing and Contracts;

1.1.6.6. Research Data;

1.1.6.7. Medical Records;

1.1.6.8. Public Safety;

1.1.6.9. Financial and Business Records

2. Management and Distribution of PII.

PII may be released only to those individuals who are authorized to use such information as part of their official ETSU duties, subject to the following requirements:

2.1.1. The PII released is narrowly tailored to a specific business requirement;

2.1.2. The information is kept secure and used only for the specific official university purposes for which authorization was obtained; and

2.1.3. The PII is not further disclosed or provided to others without proper authorization.

When necessary, PII may be provided to and handled by third parties, including cloud service providers, with the strict requirement that the information be kept secure and used for a specific official authorized business purposes as defined in applicable university contracts. Third party vendors must meet the information security qualifications established in the Higher Education Community Vendor Assessment Tool (HECVAT) and prior to PII transfer to the third party.

To the extent permitted by applicable law, exceptions to this policy may be made only upon specific request approved by the Data Custodian responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and business needs of the institution. If an exception is authorized by the appropriate Data

Custodian, the exception must be documented, retained securely, and reviewed periodically by the appropriate institutional official or designee. Exceptions may be modified or eliminated based on this review and shall be documented and retained for audit purposes.

3. Management and Distribution of Government Issued Personal Identifiers.

3.1. Social Security Numbers (SSNs)

ETSU collects SSNs when: (1) required to do so by law; (2) no other identifier serves the business purpose; (3) an individual volunteers the SSN as a means of locating or confirming personal records; or (4) in other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.

3.1.1. Release of SSN.

ETSU will release SSNs to persons or entities outside the university only:

3.1.1.1.1. As required by law;

3.1.1.1.2. When permission is granted by the individual;

3.1.1.1.3. When the external entity is acting as the university's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or

3.1.1.1.4. When the appropriate legal counsel has approved the release.

3.1.2. Use, Display, Storage, Retention, and Disposal.

SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a university official for a university business purpose. The release or posting of personal information, such as grades or occupational listings keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access. SSNs will be transmitted electronically only for business purposes approved by the university officials responsible for SSN oversight and only through secure mechanisms. The Data Custodians responsible for SSNs will oversee the establishment of business rules for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.

3.2. Non-SSN Government Issued Identifiers

During business operations, ETSU has access to collect and use non-SSN government-issued identifiers such as driver's licenses, passports, National Provider Identifiers, Employee Identification Numbers (EIN), and military identification cards, among others. ETSU shall follow the Minimum Necessary standard and safeguard these identifiers.

4. Management and Distribution of Institution Issued Identifiers.

An Institutional ID is assigned at the earliest possible point of contact between the entity and the institution. It is associated permanently and uniquely with the entity to which it is assigned. The Institutional ID is considered PII by the institution, to be used only for appropriate business purposes in support of operations. It is used to identify, track, and serve individuals across all institutional electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the institution and presence in the institution's systems or records. The Institutional ID is not to be disclosed or displayed publicly by the institution, nor to be posted on the institution's electronic information or data systems, unless the Institutional ID is protected by access controls that limit access to properly authorized individuals. The release or posting of personal information keyed by the Institutional ID, such as grades, is prohibited. Any document, item, file, or database that contains Institutional IDs in print or electronic form is to be protected and disposed of in a secure manner in compliance with data retention rules. Institutional IDs are maintained and administered by the appropriate institutional office in accordance with this policy. Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for use in accordance with this policy.

5. Responsibility for Maintenance and Access Control.

Access to electronic and physical repositories containing PII shall be controlled based on reasonable and appropriate administrative, physical, technical, and organizational safeguards. Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority. All paper documents with PII must be under lock and key or otherwise securely stored. Document retention policies dictate schedules for PII deletion and/or destruction. Proper disposal of PII must be completed in compliance with ETSU's Records Retention and Disposal policy.

6. Enforcement

Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of PII may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the institution or, in the case of students, suspension or expulsion from the university.

Policy Name: Personally Identifiable Information

Procedures

N/A

Applicable Forms and Websites

https://www.etsu.edu/reg/records/ferpa.php

Authority and Revisions

Authority: T.C.A § 49-8-203 et. Seq., Open Records Act of Tennessee, Gramm Leach Bliley Act (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; T.C.A. § 47-18-2107.

Previous Policy: N/A

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.