



Under Review

New York University

UNIVERSITY POLICIES

Title: Personally Identifiable Information Policy
Effective Date: February 10, 2009
Supersedes: *Policy on Personal Identification Numbers* (February 6, 2006)
Issuing Authority: The Provost and The Executive Vice President
Responsible Official: The Provost and The Executive Vice President

Policy

Members of the University community shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all Personally Identifiable Information (PII) irrespective of its source or ownership or the medium used to store it. All individuals who dispense, receive, and store PII have responsibilities to safeguard it.

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

- I. To enhance individual privacy for members of the University community through the secure handling of PII and personal identifiers (PIDs);
- II. To ensure that all members of the University community understand their obligations and individual responsibilities under this policy by providing appropriate training that will permit the University community to comply with both the letter and the spirit of all applicable privacy legislation;
- III. To increase security and management of Social Security numbers (SSNs) by:
 - A. inculcating broad awareness of the confidential nature of the SSNs;
 - B. establishing a consistent policy about the use of SSNs throughout the University; and
 - C. ensuring that access to SSNs for the purpose of conducting University business is granted only to the extent necessary to accomplish a given task or purpose.
- IV. To use, throughout the University, a unique University ID (UID) that serves as the primary identification element for persons associated with NYU and is applicable across the entire NYU enterprise, reducing reliance on the SSN for identification purposes.
- V. To not transmit, process, or store any complete credit card data on any University owned/controlled computers, servers, desktops, laptops, disks, flash drives, or other portable or mobile devices.

Data Trustees are responsible for oversight of personally identifiable information in their respective areas of University operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant University officials.

Purpose of this Policy

New York University creates, collects, maintains, uses, and transmits personally identifiable information relating to individuals associated with the University including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. The University is committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations in order to maximize trust and integrity.

Scope of this Policy

This policy applies to all members of the University community, including all full- and part-time employees, faculty, students and their parents or guardians, and other individuals such as contractors, consultants, other agents of the community, alumni, and affiliates that are associated with the University or whose work gives them custodial responsibilities for PII.

Policy Definitions

Data Trustees: Data Trustees (see the *University Data Management Policy*, section C.1) are senior University officials (typically at the level of Vice President or higher) who have planning and policy-making responsibilities for University data and the University Data Warehouse. The Data Trustees, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability.

Minimum Necessary: *Minimum Necessary* is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personal Identifier (PID): A PID, a sub-category of PII, is a unique code assigned to or utilized by an individual to identify that individual. PIDs are used primarily, but not exclusively, for the purpose of electronic operations. University identification numbers (UIDs) and NetIDs are examples of PIDs.

Policy Requirements

1. Data Trustees

The following are the Data Trustees who will administer this policy in their respective areas of University operations. They will resolve the responsibility for the data, if any data elements overlap more than one area.

- A. Senior Vice President for Development and Alumni Relations: Alumni and donors
- B. University Registrar: Students
- C. Associate Provost for Admissions and Financial Aid: Prospective students and applicants
- D. Vice Provost for Academic Affairs: Faculty, Visiting Scholars, Graduate/Research/Teaching Assistants, and research staff
- E. Vice President for Human Resources: Administrators, staff, service employees, and prospective employees
- F. Senior Vice President for Finance and Budget: Business Associates, consultants, contractors, and vendors
- G. Senior Vice President for Health: Patients
- H. Associate Vice Provost for Research Compliance and Administration: Research subjects
- I. Vice President for Public Safety: All other affiliated individuals, including members of the public using University resources or attending University events
- J. The Provost and the Executive Vice President: All other PII including, but not limited to, information relating to PII in intellectual property or other technology transfer or royalty, records, PII in contract and grant proposals, and surveillance tapes
- K. Vice President, Information Technology and Chief Information Technology Officer: issuance of the NetID and the security of PII in computer storage and transmission

2. Personally Identifiable Information

- A. PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official University duties, subject to the requirements:
 - (1) that the PII released is narrowly tailored to a specific business requirement;
 - (2) that the information is kept secure and used only for the specific official University [business] purposes for which authorization was obtained; and
 - (3) that the PII is not further disclosed or provided to others without proper authorization as defined above.
- B. PII may be handled by third parties with the strict requirement that the information be kept secure and used only for a specific official authorized business purpose as defined in a Business Associate Agreement with that third party.
- C. Exceptions to this policy may be made only upon specific requests approved by the cognizant University official responsible for such information as specified in this policy above and only to the degree necessary to achieve the mission and business needs of the University. Any and all exceptions made must be documented, retained securely, and reviewed periodically by the appropriate cognizant University official or his/her designee.
- D. Directory PII, as defined by Federal and State law and NYU policy, will be published following the guidelines defined by the Office of the Vice President, Information Technology and Chief Information Technology Officer.
- E. Information that has been collected that conforms to the HIPAA standards of deidentification or anonymization is not PII.

3. Government-Issued Personal Identifiers

A. Social Security Number

(1) Provision of Information

- a. NYU collects SSNs:
 - i. when it is required to do so by law;
 - ii. when no other identifier serves the business purpose; and
 - iii. when an individual volunteers the SSN as a means of locating or confirming personal records.
- b. 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.
- c. SSN collection must be approved by the appropriate campus official (see the Policy section above). When an SSN is requested, NYU informs the individual what uses will be made of the SSN and whether the disclosure is voluntary, or, if it is mandatory, by what authority.

(2) Release of SSNs

SSNs will be released by NYU to persons or entities outside the University only:

- a. as required by law;
- b. when permission is granted by the individual; or
- c. 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
- d. when the NYU Office of General Counsel has approved the release.

(4) Use, Display, Storage, Retention, and Disposal

- a. SSNs or any portion thereof will not be used by NYU to identify individuals except as required by law or with approval by a cognizant University official for a University business purpose.
- b. 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.
- c. SSNs will be transmitted electronically only for business purposes approved by the campus officials responsible for SSN oversight and only through secure mechanisms approved by the Office of the Associate Provost/Chief Information Technology Officer.
- d. The Data Trustees who are 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.

B. Non-SSN Government-Issued Identifiers

In the course of its business operations, NYU has access to, collects, and uses non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers, Employee Identification Numbers (EIN), and military identification cards, among others. NYU follows the Minimum Necessary standard and strives to safeguard these identifiers.

4. New York University-Issued Identifiers

A. University ID Number

(1) Assignment Eligibility and Issuance

- a. The UID is a unique alphanumeric identifier assigned by the University to any member of the University community who requires an identifying number in any University system or record.
- b. A UID is assigned at the earliest possible point of contact between the individual and the University.
- c. The UID is associated permanently and uniquely with the individual to whom it is assigned.

(2) Use, Display, Storage, Retention, and Disposal

- a. The UID is considered PII by the University, to be used only for appropriate business purposes in support of University operations.
- b. The UID is used to identify, track, and serve individuals across all University electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the University and presence in the University's systems or records.
- c. The UID is not to be disclosed or displayed publicly by the University, nor to be posted on University electronic information or data systems unless the UID is protected by access controls that limit access to properly authorized individuals.
- d. The UID is imprinted and encoded on the official University photo identification card known as the NYUCard. The NYUCard is the principal means of physical identification at the University, and the use of the NYUCard by the cardholder, whether by physical display or when swiped at an electronic reader, will constitute a voluntary disclosure of the UID.
- e. The release or posting of personal information keyed by the UID, such as grades, is prohibited.
- f. Any document, item, file, or database that contains UIDs in print or electronic form is to be protected and disposed of in a secure manner.

B. NetID

(1) Assignment Eligibility and Issuance

- a. The NetID is a unique alphanumeric assigned by the University to an individual.
- b. The NetID is assigned to all persons who may require access to electronic services at the University, including students, faculty, alumni, administrators, staff, service employees, and other individuals (such as contractors, consultants, and affiliates) associated with the University.
- c. The NetID is permanently and uniquely associated with the individual to whom it is assigned.
- d. The NetID, alone, without a password, will not be used for access to NYU's electronic network.

(2) Use, Display, Storage, Retention, and Disposal

- a. The NetID is used, in conjunction with an individually set password, as an authenticated identifier for on-line transactions and may be used, in addition to the UID, to identify and track individuals within the University systems, applications, and business processes.
- b. Each member of the University community will be held fully responsible for any activity authorized by that individual's NetID and password.
- c. Under the Family Educational Rights and Privacy Act (FERPA), the NetID may be used as directory information as long as the identifier cannot be used standing alone (i.e., without a password) by unauthorized individuals to obtain sensitive, non-public (i.e., non-directory) information about an individual from education records.
- d. The release or posting of personal information keyed by the NetID, such as grades, is prohibited.

C. Local User ID Numbers

In addition to University Identification Numbers (UIDs) and NetIDs, NYU schools and departments may issue other system-unique identifiers. NYU follows the Minimum Necessary standard and strives to safeguard these identifiers.

5. Other Externally-Assigned Identifiers and Other Personally Identifiable Information

NYU has access to, collects, and uses various externally-assigned identifiers other than those indicated above in the course of its business operations. These identifiers include, but are not limited to credit and debit card numbers and bank account numbers. NYU follows the Minimum Necessary standard and strives to safeguard these identifiers.

6. Responsibility for Maintenance and Access Control

- A. The University-wide UIDs and NetIDs are maintained and administered by NYU Information Technology Services (ITS). Other University offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.
- B. Access to electronic and physical repositories containing SSNs, UIDs, and NetIDs will be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.
- C. Individuals who inadvertently gain access to a file or database that contains SSNs or UIDs for which they have not been authorized shall report it immediately to ITS Technology Security Services: security@nyu.edu.

7. Enforcement

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

Related Policies and Additional Information

- NYU Guidelines for compliance with the Family Educational Rights and Privacy Act (FERPA) (www.nyu.edu/apr/ferpa.htm)
- NYU Information Technology Services Policies (www.nyu.edu/its/policies)
- NYU HIPAA Information Security Policies (<http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/hipaa-policies.html>)
- Policy on Responsible Use of NYU Computers and Data (<http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/responsible-use-of-nyu-computers-and-data-policy-on.html>)
- Data and Computer Security Policy
- Reference for Data and System Classification
- Data and System Security Measures
- Security Guidelines for Desktop and Laptop Computers
- Security Guidelines for System Administrators
- NYU Data Classification Table (www.nyu.edu/its/policies/data-classification.html)
- University Data Management Policy
- Guidelines on equipment disposal or redeployment (www.nyu.edu/asset) and (www.nyu.edu/its/security/disposal.html)
- E-mail address for computer security assistance and advice (security@nyu.edu)
- For policy clarifications and suggestions and to report policy violations, contact the IT Service Desk (www.nyu.edu/its/askits/helpdesk/)

History of Amendments

- A. February 10, 2009: The NYU Identity and Access Management Steering Committee reviewed the *Policy on Personal Identification Numbers*, broadened it to include all personally identifiable information, and approved the amended policy now known as the *Personally Identifiable Information Policy*.
- B. April 28, 2011: First revision - supersedes policy effective February 6, 2006.