

# Social Security Number (SSN) and Unique Person Number Usage (UPN) Policy

Effective Date: September 10, 2007

## Policy Statement

The University's policy is to protect Social Security Number (SSN) or equivalent data from unauthorized or unnecessary disclosure.

## Reason(s) for the Policy

Federal and state statutes require handling SSNs in the most confidential manner. The distinctiveness of the SSN as an individual identifier makes it increasingly vulnerable to exploitation. Identity theft and the compromise of personal information are a growing concern for many institutions. The purposes of this policy are to:

- generate broad awareness of the confidential nature of the SSN;
- provide consistent and clear guidelines for acquisition and use of SSN data;
- eliminate unnecessary storage and use of SSNs in University documentation, practices and systems;
- eliminate the use of the SSN as the primary identifier at the University; and
- define the use of Unique Person Number (UPN) as the new alternate individual primary identifier in University systems and practices.

## Primary Policy to Which This Policy Responds

This policy responds to all applicable federal and state statutes pertaining to use of Social Security Numbers. These statutes include, but are not limited to, the New York State Law, the New York State Information Security Breach and Notification Act, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Gramm-Leach-Bliley Act (GLBA).

## Responsible University Officer and Office

Compliance Responsibility: Office of the General Counsel  
Policy Maintenance and Technical Support: Columbia University Information Technology (CUIT) and Security Office

## Revision History

This policy is established in June 2007 (Initial Draft).

## Who is Governed by This Policy

This policy applies to all individuals who access, use, or control information technology and/or non-electronic records containing SSN information. The individuals covered include, but are not limited to, faculty, staff, students, and those working on behalf of the University.

## Who Should Know This Policy

All individuals listed above, particularly the custodians of SSN data.

## Exclusions & Special Situations

None

### Policy Text

The University is committed to safeguarding the security and confidentiality of personal and confidential information in compliance with applicable laws. The use of the SSN as a primary identifier shall be avoided, except as required by law or as required by the business necessity. In order to protect the SSN of its faculty, staff, students and other individuals associated with the University, Columbia University will:

1. Discontinue the collection of SSN except where necessary for employment records, financial aid records, health records and other business and governmental transactions as required by law or to satisfy a business requirement.
2. Develop a Unique Person Number (UPN) to uniquely and permanently identify individual faculty, staff, students and others associated with the University. The UPN will be used in lieu of the SSN and be assigned and distributed to the individual upon initial association with the University. It will be used in all electronic and paper data systems to identify, track and service the individual.
  - 2.1. The UPN will be considered the property of Columbia University, and its use and governance shall be at the discretion of the University, within the parameters of the law;
  - 2.2. The UPN will be maintained and administered in accordance with Columbia University policy on the Unique Personal Number;
  - 2.3. The UPN will be a component of a system that provides a mechanism for the public identification of individuals
  - 2.4. All services rendered by Columbia University and electronic business systems will rely on the identification and authentication services provided by this system.
3. Ensure that no new systems or technology will be purchased or developed by Columbia University that use the SSN as its primary key to the database except where required by law. Any exemption to this policy must be approved by Offices of CUIT, Chief Information Security Officer and General Counsel.
4. Ensure that new systems or technologies purchased or developed by the Columbia University will only use SSNs as data elements (not as database keys) when required by law or business necessity.
5. Ensure that any request (verbal or written) for SSN data of employee, faculty, staff or students is for the legitimate purpose indicating intended use of such information.
6. Ensure that the SSN is blanked out of any document or form requested when the SSN is not relevant to the request. In addition, the response should include a statement indicating that the SSN is not required.
7. Ensure that no new systems purchased or developed by Columbia University display SSN visually, whether on computer monitors or on printed forms or other output, unless required by law or business necessity.
8. Develop an implementation plan to ensure compliance with this policy for existing systems.
9. Assure transactions involving SSN and UPN will be conducted in a secure manner.
10. SSN data and UPN data shall be protected at all stages (i.e., in storage, in transit, and in backups).

## **Compliance**

An employee, student, volunteer, representative, contractor, or any other agent of Columbia University who has substantially breached the confidentiality of SSNs may be subject to disciplinary action or sanctions up to and including discharge or dismissal in accordance with University policy and procedures.

Unauthorized use of SSN is a serious criminal offense. The penalties may be as severe as suspension or dismissal from the University and/or criminal prosecution. Violation may also result in criminal prosecution. It is a felony, punishable by up to 5 years in prison, to compel a person to provide a SSN in violation of Federal Law.

## **Definitions**

**Social Security Number (SSN)** may be interpreted to include Taxpayer Identity Number (TIN).

**Unique Person Number (UPN)** is created as a 9-digit system-to-system identifier by the Columbia University Identity Management (IDM) System. The UPN shall be assigned to each faculty member, employee or student as a unique attribute / primary identifier,. The UPN has no intrinsic value except as an identifier internal to Columbia.

## **Appendix**

### **References**

- NY State Law: Chapter 16, Article 1, Title 1, Section 2b  
<http://caselaw.lp.findlaw.com/nycodes/c30/a3.html>
- Gramm-Leach-Bliley Act (GLBA)  
<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>
- Family Educational Rights and Privacy Act (FERPA)  
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- Health Insurance Portability and Accountability Act (HIPAA)  
[http://www.cms.hhs.gov/HIPAAGenInfo/02\\_TheHIPAALawandMore.asp](http://www.cms.hhs.gov/HIPAAGenInfo/02_TheHIPAALawandMore.asp)
- The Immigration and Control Act of 1986 (IRCA)  
<http://www.oig.lsc.gov/legis/irca86.htm>  
[http://www.dol.gov/esa/regs/compliance/ofccp/ca\\_irca.htm](http://www.dol.gov/esa/regs/compliance/ofccp/ca_irca.htm)
- Social Security Act of 1935  
<http://www.nationalcenter.org/SocialSecurityAct.html>

### **Governing Laws**

The following are examples of major laws for protection, usage, and disclosure of personal information, including SSN:

NY State Law: Chapter 16, Article 1, Title 1, Section 2b (excerpt)

Use of student social security numbers is restricted. No public or private elementary or secondary school or college as defined in section two of this article shall display any student's social security number to identify such student for posting or public listing of grades, on class rosters or other lists

provided to teachers, on student identification cards, in student directories or similar listings, or, unless specifically authorized or required by law, for any public identification purpose.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).

FERPA protects the privacy of student educational records and requires schools to minimize collection and use of student Social Security Numbers. Social Security Numbers should be collected only for the purpose of processing student loans, employment, and to meet other legal obligations.

The Gramm-Leach Bliley Act (GLBA) [aka Financial Services Modernization Act of 1999]

The GLB Act governs the collection, safeguarding, and disclosure of customers' personal financial information.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPPA requires securing all protected health information (PHI). It establishes standards for information privacy, electronic transactions, security, and unique identifiers for individuals.

**Below are some examples of appropriate purposes for using SSNs that are currently approved:**

1. Tax Reporting – An SSN is required as a taxpayer ID for all tax information reported to the IRS, including wage and withholding data for full-time and part-time faculty, staff, and students, for honoraria provided to guest lecturers, and for individuals working for the University as independent contractors.
2. Financial Aid – An SSN is necessary to obtain financial information and to identify and confirm the level of financial aid assistance.
3. Human Resource Services - The Immigration Reform and Control Act of 1986 (IRCA) requires the use of an SSN for I-9 forms, and certain benefit providers, such as health insurance companies, may require an SSN for verification of eligibility and coordination of benefits. Therefore, in addition to the tax reporting reasons, SSNs will need to be collected from all new employees in the new hire process, and may be requested and used for certain human resource services functions when necessary.
4. Law Enforcement – Federal and state agencies often rely upon SSNs as the primary identifier for law enforcement and criminal information purposes. In the event such agencies request SSN information using proper procedures, and the University has such information, it will be provided following review and approval by the Office of the Vice President and General Counsel.