1.6.1 PRIVACY POLICY

Last updated on: 03/15/2013

Formerly Known As Policy Number:
16.1

Stanford University has an interest in ensuring that the privacy of its students, faculty, and staff is respected. The University is committed to protecting the privacy of Prohibited, Restricted and Confidential Information within its control in a manner consistent with applicable laws, regulations and University policies.

Authority:
Approved by the Vice President for Business Affairs and CFO.

Applicability:
This policy is applicable to all members of the Stanford community and visitors to the University, including but not limited to students, post doctoral scholars, faculty, lecturers/instructors, staff, third-party vendors, and others with access to Stanford's campus and University Prohibited, Restricted and Confidential Information.

1. Definitions

a. Disclosure: "Disclosure" is the release of, transfer of, provision of access to, or other communication of Information outside of the Stanford community.

b. Use: "Use" is the examination, sharing, or other utilization of Information within the Stanford community.

c. Information: "Information" is all Stanford University Prohibited, Restricted and Confidential information, whether in electronic or paper format, defined in Stanford's Data Classification, Access, Transmittal and Storage Guidelines [1].


2. Information Privacy
a. General Policy
Stanford should limit the collection, use, disclosure or storage of Information to that which reasonably serves the University’s academic, research, or administrative functions, or other legally required purposes. Such collection, use, disclosure and storage should comply with applicable Federal and state laws and regulations, and University policies.

b. Legal and University Process
Notwithstanding the General Policy contained in section 2.a, the University may disclose Information in the course of investigations and lawsuits, in response to subpoenas, for the proper functioning of the University, to protect the safety and well-being of individuals or the community, and as permitted by law.

c. Policies That Apply to Special Categories of Information
Stanford has adopted policies governing certain categories of Information. These policies are listed in this section, 2.c. To the extent that there is a conflict between this Administrative Guide Memo 16.1 and any of these special policies, the special policy will control. For more information about Stanford’s compliance with any of the laws and policies referenced below, please contact the University Privacy Officer at privacyofficer@stanford.edu or the individual listed in section 4.b as responsible for compliance.

(1) Prohibited Information, including Social Security Number (“SSN”) and Drivers License Number (“DLN”)
Stanford should not use an individual’s SSN or DLN as a personal identifier unless required by law or approved by Stanford’s Vice President for Business Affairs and Chief Financial Officer or the Data Governance Board. Prohibited information, including SSNs and DLNs, may be stored electronically only in compliance with the Guidelines. If Prohibited Information must be stored on paper, the files must be stored securely with access provided only to authorized persons.

(2) Student Records
Students have rights with respect to access to their education records under the Family Educational Rights and Privacy Act of 1974 (“FERPA”). These rights are outlined in the Stanford Bulletin.

(3) Health Information
Individuals have rights with respect to the privacy and security of their health information under Federal and state laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). These rights are outlined in Guide Memo 1.6.2 and in the University health information privacy policies that can be found at the HIPAA website.

(4) Human Subjects Research Information
In addition to the rights afforded by HIPAA and other laws related to health information, the Federal Policy for the Protection of Human Subjects (“Common Rule”) outlines provisions specific to the privacy of research participants and the confidentiality of their information. The Stanford Research Compliance Office maintains the Human Research Protection Program (“HRPP”) that includes the University policies related specifically to human subjects’ research information.

(5) Financial Services Records
The Gramm-Leach-Bliley Act (“GLBA”) requires that Stanford protect the privacy and security of information collected in the course of providing certain financial services, such as student financial aid or faculty staff housing loans. Stanford has adopted polices to protect this information. These policies are located on the Office of General Counsel’s website.

(6) Information Collected in the Course of Electronic Commerce
Some areas of the Stanford website operate commercial enterprises online. Stanford also delivers online service through its network. To comply with the California Online Privacy Protection Act of 2003 when
Stanford (or any of its partners) collects personally identifiable consumer information on one of the commercial areas of its website or as the operator of an online service, it will conspicuously post either a privacy policy or a link to a privacy policy on the portal page for the commercial activity. This policy will:

(a) Identify the categories of personally identifiable information collected through the commercial portions of its website or through its online service;
(b) Identify the categories of third-parties with whom Stanford may share that personally identifiable information;
(c) Provide a description of how an individual may request changes to their personally identifiable information collected through the Web site or online service and retained by Stanford, if any process exists;
(d) Describe the process by which Stanford will notify users of the commercial portion of Stanford's website or its online service of material changes to the Stanford's privacy policy for that portion of the website or online service (it is sufficient to say that the policy will be updated online); and
(e) Identify the effective date of the privacy policy and all updates.

d. Confidentiality Agreement
Members of the Stanford community are subject to the Confidentiality and Privacy provisions set forth in Section 3 of the Code of Conduct contained in Administrative Guide Memo 1. As a reminder of Stanford's commitment to privacy, students, faculty, staff and other members of the workforce may be asked to sign a confidentiality statement based on the Code of Conduct and this privacy policy. Failure to sign such a statement in no way diminishes the obligation to uphold Stanford's policies.

e. Training
Departments within Stanford University are responsible for ensuring that all members of their workforce (including, among others, faculty, staff, students, consultants and volunteers) receive appropriate training on Stanford's privacy and security policies to the extent necessary and appropriate for them to carry out their required job functions. Departments will maintain adequate records of workforce training, which will be provided upon request by the Office of the General Counsel, the University Privacy Officer, the Chief Information Security Officer, Internal Audit, Human Resources or other University official with a reasonable Stanford-related need for the information.

3. Expectation of Privacy

a. General Policy
Stanford respects and values the privacy of its faculty, students and staff and will not monitor its community members without cause except as required by law or as permitted by the policies and agreement referenced below:

- **Computer and Network Usage.** See section 2.c in Guide Memo 6.2.1 [13]: Computer and Network Usage Policy.
- **Library Circulation Records.** See Stanford University Libraries policy on Disclosure of Borrower Information [14].
- **University Student Housing.** See Stanford residence agreement terms [15] for limited circumstances in which student residences may be accessed.

b. Photography and Recording on Campus
In order to protect the privacy of the Stanford community, photographs, video recordings and other recordings
may be made only in accordance with University policies on campus photography [16].

c. Visitors on Campus
The University is private property; however, some areas of the campus typically are open to visitors. These areas include White Plaza, public eating areas, retail establishments, outdoor and indoor guided touring areas, roads, walkways, designated parking areas and locations to which the public has been invited by advertised notice (such as for public educational, cultural, or athletic events). Even in these locations, visitors must not interfere with the privacy of students, postdoctoral scholars, faculty, lecturers/instructors, and staff, or with educational, research, and residential activities. The University may revoke at any time permission to be present in these, or any other areas. Visitors should not be inside academic or residential areas unless they have been invited for appropriate business or social purposes by the responsible student, post doctoral scholar, faculty member, lecturer/instructor, or staff member.

4. Responsibilities

a. University Privacy Officer
The University shall have a Privacy Officer who is responsible for:
(1) Interpreting this Administrative Guide Memo 1.6.1;
(2) Providing advice with a view to encouraging compliance with all privacy laws and regulations, improving privacy practices, and resolving problems;
(3) Establishing privacy policies and procedures in areas not covered by section 5.c below.
(4) Recommending privacy policy and policy changes in all areas related to privacy at Stanford;
(5) Chairing the Data Governance Board; and
(6) Facilitating special privacy-related situations.

In order to discharge these responsibilities, the University Privacy Officer will collaborate with Stanford's Chief Information Security Officer, the General Counsel, other University privacy officials and other University administration, as appropriate.

b. Establishing Privacy Policies and Procedures
The University has designated certain officials with primary responsibility for establishing policies and procedures governing University compliance with certain specific privacy laws and regulations:

- FERPA. The University Registrar has primary responsibility for establishing policies and procedures related to compliance with the Family Educational Rights and Privacy Act.
- HIPAA. The University Privacy Officer has primary responsibility for establishing policies and procedures related to compliance with the Health Insurance Portability and Accountability Act of 1996 for Stanford's Affiliated Covered Entity;
- GLBA. The University Privacy Officer has primary responsibility for establishing policies and procedures related to compliance with the Gramm-Leach-Bliley Act.

c. Information Custodians and System Owners
Each individual who retains custody of Information, and each system owner, is responsible for the application of this Guide Memo1.6.1 [17] and all related University policies to the systems and Information under their care or control.
5. Violations of this Policy

a. Failure to follow proper policies and procedures concerning access, storage and transmission of Information may result in sanctions and disciplinary action up to and including termination of employment, referral to Judicial Affairs or other applicable administrative process.

b. Members of the Stanford community who believe that these policies have been violated should report such violations to the University Privacy Officer, Office of the University Ombuds, Internal Audit or Office of the General Counsel. Complaints or concerns may also be reported anonymously by calling the University Compliance Officer at (650) 721-2667 or reporting it online [18].

c. Any School or Department found to have violated this policy may be held accountable for the financial penalties and remediation costs that are a direct result of this failure.

Back to top

6. Relevant Laws


d. Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. Law 104-191) and HIPAA regulations, including but not limited to the HIPAA Privacy Rule and HIPAA Security Rule, 42 CFR Parts 160, 162, 164

e. Health Information Technology for Economic and Clinical Health (HITECH) Act (H.R.1, 2009, Sec. 13001 et seq.) and related regulations, including but not limited to:
   

f. California breach notification law (businesses), CA Civ. Code 1798.8

g. Confidentiality of Medical Information Act, CA Civil Code 56 et seq.

h. Employee Health Information Privacy, CA Civ. Code 56.20

i. Lanterman Petris Short Act, CA W&I Code 5328 et seq.

j. Patient Access to Health Records Act, CA H&S 123100-123149.5

k. HIV Privacy, CA H&S 121010 et seq., 121075 et seq., CA Penal Code 12020.1, 1524.1

Back to top
7. Related Stanford Policies

a. **Student Discipline** — See Student Life/Codes of Conduct/Fundamental Standard/Honor Code
b. **Staff Discipline** — See Administrative Guide Memo 2.1.16 [20]: Addressing Conduct and Performance Issues
c. **Faculty Discipline** — See the Statement on Faculty Discipline
d. **Computer and Network Usage** — See Administrative Guide Memo 6.2.1 [13], Computer and Network Usage Policy
e. **Privacy Incident Response** — See Administrative Guide Memo 6.6.1 [21]: Information Security Incident Response [22]; HIPAA Policy, Breach Notification Policy for Incidents Involving Electronic and Non-Electronic PHI
f. The policies identified in sections 1, 2 and 3 of this Administrative Guide Memo 1.6.1 [17].

Back to top