

OFFICE OF HUMAN RESOURCES DEVELOPMENT & SERVICES

SLAC MEMORANDUM

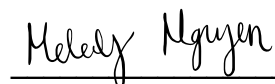
TO: Summer Interns
FROM: Carolyn Nelson, Director of Human Resources Development & Services
DATE: March 24, 2021
SUBJECT: Confidentiality Expectations and Agreement

In light of privacy laws, I am writing to formally remind you that in your position at SLAC, you are entrusted with confidential and sensitive information pertaining to SLAC and Stanford University. Much of this information is required to be kept confidential in accordance to the Federal and State privacy laws. This information includes, but is not limited to personal, medical, and financial data. It is essential that you keep this private or legally protected information confidential and that you use care so that it is not accidentally or intentionally disclosed.

Handling and disposal of confidential and private information must be done in ways that ensures it is not inappropriately or inadvertently disclosed or available to others. Please do not leave confidential information in public view on your desk or in a similar visible place. Hard copies of confidential information should be shredded when you are through working with them.

For more information, please review the following Administrative Guide Memos: *University Code of Conduct*, found at: <https://adminguide.stanford.edu/chapter-1/subchapter-1/policy-1-1-1>, *Staff Policy on Conflict of Commitment and Interest*, found at: <https://adminguide.stanford.edu/chapter-1/subchapter-5>, and *Information Security*: <https://adminguide.stanford.edu/chapter-6/subchapter-3>. Pages 2 and 3 summarizes the most pertinent content of those guide memos. **You are expected to review and maintain current knowledge of Stanford University and any SLAC institutional policies regarding use and handling of confidential information.**

Your signature below acknowledges that you have carefully read and fully understand the importance of the above work instruction and agree to follow it. You also understand that failure to abide these policies may result in serious disciplinary action and could impact your position at SLAC.

Summer Intern Printed Name

Summer Interns Signature

Date

Confidentiality Expectations and Agreement Policy Attachments

This document summarizes the most pertinent content of Stanford University Administrative Guide Memos (AGM), which address the confidentiality of information. The complete policies can be found at: <https://adminguide.stanford.edu/chapters>

AGM 1.1.1, University Code of Conduct, Section 5:

University Community members receive and generate various types of confidential, regulated, proprietary and private information on behalf of the University. All members of the Community are expected to comply with all applicable rules, laws, and regulations (whether federal, state, local or foreign), contractual obligations, and University policies pertaining to the use, protection and disclosure of this information. When disaffiliating from Stanford, University Community members must return all sensitive University data unless an exception has been granted.

AGM 1.5.2, Staff Policy on Conflict Commitment and Interest, Section 2.b:

Confidential or Privileged Information-

Using for personal gain or other unauthorized purposes, confidential or privileged information acquired in connection with the individual's University-supported activities. Confidential or privileged information is non-public information pertaining to the operation of any part of the University including, but not limited to, documents so designated, medical, personnel, or security records of individuals; anticipated material requirements or price actions; knowledge of possible new sites for University-supported operations; knowledge of forthcoming programs or of selections of contractors or subcontractors in advance of official announcements; and knowledge of investment decisions. Questions about confidential information may be referred to the University Privacy Officer at privacyofficer@stanford.edu

AGM 6.3.1, Information Security, Section 4:

Violations of Policy and Misuse of Data-

Violations of this policy include, but are not limited to: accessing information to which the individual has no legitimate right; enabling unauthorized individuals to access information; disclosing information in a way that violates applicable policy, procedure, or other relevant regulations or laws; inappropriately modifying or destroying information; inadequately protecting information; or ignoring the explicit requirements of Data Owners for the proper management, use, and protection of information resources.

Violations may result in network removal, access revocation, corrective action, and/or civil or criminal prosecution. Violators may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to campus policies, collective bargaining agreements, codes of conduct, or other instruments governing the individual's relationship with the University. Recourse shall be available under the appropriate section of the employee's personnel policy or contract, or by pursuing applicable legal procedure.

- a.** Any School or Department found to have violated this policy may be held accountable for the financial penalties and remediation costs associated with a resulting information security incident.
- b.** Third party vendors found to have violated this policy may incur financial liabilities, in addition to termination of contract.

Patent and Royalty Rights

I hereby state that to the best of my knowledge and belief,

- 1) I do not own or control,
- 2) Nor have I owned or controlled,
- 3) Nor am I entitled to receive royalties for

Any invention or patent, either applied for or granted, in the accelerator field and which may be used in the design, construction, and/or operation of the National Facility operated by Stanford University at SLAC National Accelerator Laboratory, except as noted below:

Note:

- a.) For each invention or patent noted above, please include the U.S and/or Foreign Patent No., title, date of expiration, and, if different from that of the person signing this statement, the name of holder of legal title.
- b.) If you have owned or controlled a patent which would qualify under the cited criteria, but have disposed of it in the past, list the present patent owner (if known), together with the required information as stated above and indication of the date you disposed of it.
- c.) If you have not owned or controlled a patent or invention that qualifies under the criteria stated above, write "none."

I certify that the above information is complete and accurate.



Signature

Date

Print name

Personally Identifiable Information (PII) SLAC Individual Certification

POLICY: SLAC policy PROHIBITS employees from saving Personally Identifiable Information (PII) on desktops, on laptops, or personal storage devices unless the information is encrypted. SLAC policy also prohibits transmitting PII through email unless masked or encrypted.

DEFINITION: Personally Identifiable Information, in conjunction with a person's name, includes:

- * Social security numbers
- * Credit card numbers
- * Financial account numbers, such as checking or investment accounts
- * Driver's license numbers
- * Health insurance policy identification numbers

RESTRICTED AND CONFIDENTIAL INFORMATION: All employees are responsible for protecting RESTRICTED and CONFIDENTIAL information per Stanford policy and in compliance with state and federal laws and regulations.

RESTRICTED INFORMATION is limited to access to those permitted under law, regulations, Stanford, and SLAC policies with a need to know. Restricted Information includes:

- * Passport and Visa numbers
- * Student Records
- * *Dual Use* Export Controlled Information
- * Research and other information covered by non-disclosure agreements
- * Protected Health Information, such as medical records or biometric information

SLAC employees, who have a need to know the above listed information, may store such data on the secured OneDrive.

CONFIDENTIAL INFORMATION is information not generally available to the public or to other employees without a legitimate business reason. CONFIDENTIAL INFORMATION would include personnel actions and personal information, among other things:

- * Salary, performance appraisals, disciplinary actions and other memos of a sensitive or confidential nature, and attorney-client communications
- * Personal information, such as birth date, benefits information, or personal contact information

The OneDrive should be used exclusively for Restricted and Confidential data. If you do not see the drive ask your Department Support Admin for assistance.

Unauthorized use or release of PII may be subject to criminal prosecution and/or civil liability. In addition, employees will be subject to disciplinary action, up to and including termination, or in the cases of subcontractors, immediate removal from any and all work conducted or performed for SLAC.

Personally Identifiable Information (PII) SLAC Individual Certification

1. I understand that Personally Identifiable Information (PII) on SLAC staff members, users, or visitors to SLAC is to be carefully protected due to the potential risks for misuses such as identity theft.
2. I have read through the list of examples of Personally Identifiable Information (PII) listed in the Individual Certification.
3. I agree that if I find PII data stored on my hard or shared drives, or know of any unauthorized release of PII, I will contact the Human Resources Director of SLAC immediately.
4. Please check the box that applies:

I do not have and have never had any PII on SLAC staff members, users, or visitors either on computers, removable storage devices, PDA's or similar devices, CD's or other such media, or on paper.

I have had in the past, but no longer have, PII on SLAC staff members, users, or visitors either on computers, removable storage devices, PDA's or similar devices, CD's or other such media, or on paper. I certify that no PII remains in my possession either in paper or electronic form.

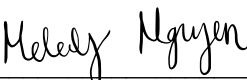
I may currently have or may in the future in my possession PII on SLAC staff members, users, or visitors either on computers, removable storage devices, PDA's or similar devices, CD's or other such media, or on paper. I need to review what I may possess more carefully and/or clarify the PII definition with my supervisor before determining whether or not I possess PII.

I do not know if I currently have in my possession PII on SLAC staff members, users, or visitors either on computers, removable storage devices, PDA's or similar devices, CD's or other such media, or on paper. I will require assistance in order to make such a determination.

5. I agree as a condition of being a custodian for PII, should I possess it either now or in the future, that I will use reasonable care to protect it from abuse or unauthorized access or use. I will keep all devices, components, media, and paper that contain PII locked or secured in a suitable fashion. I understand that only shredding of paper documents and physical destruction or special software that overwrites the data on electronic media is sufficient to eliminate PII from devices under my supervision.
6. I agree that if my access to PII changes to where I become a custodian for PII, that I will complete and sign an updated SLAC PII Certification Form.

After reviewing the information above, please sign this document and return it to Human Resources.

Name (print)



Signature

Date