

## STUDENT EMPLOYEE CONFIDENTIALITY POLICY

(Adopted 8/07)

### I. Policy

Students may be employed by the University under a variety of circumstances—administrative assistants, teaching assistants, tutors, research assistants, resident assistants, coaches, work study positions, and others—and also may serve on numerous committees that expose students to confidential or sensitive information. Student employment and participation on committees and other governance entities benefits both the student and the University. From an organizational perspective, the University’s reputation and effectiveness depend on the ability and intention of all employees to manage our data and records with care and discretion.

Managing the affairs of a university requires a wealth of information, which must be free to flow efficiently among those who need it to fulfill their responsibilities. However, students—like the employees beside whom they work—are accountable for safeguarding the privacy of the University’s employees, students, and external constituents. Regardless of its form (electronic, oral, written), information *must* be handled according to standards that are legal, ethical, and responsible.

For example, University employees are subject to provisions of these federal laws:

- Family Educational Rights & Privacy Act (FERPA)
- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA).

There are additional regulations at the state level, as well as rules that govern educational institutions, financial aid administrators, student athletics administrators, personnel administrators, and so on. Violations of these provisions by student employees endanger both the student and the University. More fundamentally, using information for unintended purposes, or publicizing information carelessly or maliciously, is simply wrong; such acts violate the trust we place in our employees to conduct themselves professionally and responsibly.

This document is intended to provide *basic* guidance to student employees and their supervisors in accessing and handling sensitive information. More detailed guidelines that apply to specific offices are available from office supervisors. Student employees must read and understand this document, and sign the form on the last page, before a Work Authorization Card will be issued. The form will be filed in the Financial Aid Office.

## **II. Guidelines for Safeguarding Confidential Information**

These general guidelines apply to the release of data and personally identifying information, regardless of its form:

1. Data regarding students, employees, finances, and operations should not be provided to non-University employees without your supervisor's permission. Some data are routinely provided to non-UNH constituents—your supervisor will instruct you on the proper handling of such information.
2. Data regarding students or employees should not be provided to the students or employees themselves, without authorization from one's supervisor. Some information is provided routinely—your supervisor will instruct you on the proper handling of such information.
3. Information regarding a student can be revealed to specific individuals within the university (including other students) only on a strict "need to know basis" and should not be provided to the student's parents or guardians or to any other individual outside the university without the student's signed "*Student Release – University Records and Information Form.*" Your supervisor will instruct you on how to safeguard the privacy of student information as governed by university and government policy.
4. Information available to student employees or committee members through their University positions may not be used for personal gain, to provide 'favors' for friends or others, or for any other unintended use.

### **A. Types of Information That May Be Sensitive or Confidential**

The following is a non-exhaustive list of types of information that may be governed by statute or by University policy, or that could be sensitive if mishandled:

- Any records from Matrix concerning students, faculty, staff
- Student and employee disciplinary records
- Financial Aid records
- Employment records and other data maintained by Human Resources
- Student and employee health records
- Telephone messages
- Home or cell telephone numbers
- Employee or student addresses
- Social Security numbers or other personally identifying data
- Student visa status or other immigration information
- Employee electronic calendars or contact information
- Email addresses
- Minutes or other records of confidential bodies (*e.g.*, grievance or disciplinary committees of which students are members)
- Private conversations conducted in one's office area

## **B. Guidelines for Use of University Computers and Data Systems**

1. *Unattended Machines.* Desktop computers left unattended for more than a few minutes should be locked down, so that a password log-in is required for their continued use. Computers should be locked down or turned off at the end of the day.
2. *Secure Access.* Password access to computers or campus systems should be provided to students with great discretion, and on a “need-to-know” basis.
3. *Setting Passwords.* Passwords used to access University computers or systems should be set by office supervisors and should not be changed by others. Any required changes in passwords must be approved by the supervisor.
4. *Remote Access.* Access to University systems and computers from remote locations (home, classrooms, dorms, etc.) by student employees should not occur, except with explicit instruction by supervisors. Such access will be exceedingly rare, and will be in response to extraordinary need.
5. *Personal Use of University Machines.* University computers and technology provided to student employees to perform their jobs should not be used for personal use. Installation of non-UNH applications and hardware is strictly forbidden.

## **C. Guidelines for Handling Files and Records**

1. *Removal of Files.* Student employees should not remove paper files, printouts, diskettes, compact discs, DVDs, flash-drives, or other records from the office where they are used without explicit instruction from the supervisor.
2. *Offloading files.* Files should not be downloaded to the student’s laptop, PDA, or other mobile device without instruction to do so. All files transported off of University systems should be password protected and/or properly encrypted.

## **D. Guidelines for Access to University Offices**

1. *Access “After Hours.”* Student employees are not to enter University offices during hours the offices are not open, unless specifically instructed to do so by their supervisors. Campus Police must be notified in writing if students will have access to offices without supervision.
2. *Access by Non-Employees.* Students who are not employed in a given office are not permitted in secure areas of that office without permission by the office supervisor. Students not employed in the office should not be permitted by computers or other file locations where sensitive information may be seen.

### **III. General Procedures Supporting This Policy**

#### **A. What is Proper Procedure for Handling Information?**

*Seeking Guidance on Proper Procedure.* Each office will have information relevant to its duties on the proper handling of sensitive data and other information. Further guidance is available on our website regarding our computer systems. The rule of thumb in all cases, however, is simple—if you are in doubt, ask your supervisor for guidance.

#### **B. Reporting Violations**

1. *Reports by Students.* It is important that violations of this information management policy are addressed. If you witness others acting in a way that is contrary to this policy, you are to report your suspicion to your supervisor. If the suspected violation occurs in an office other than your own, you may report your suspicion to the supervisor of that office.
2. *Failing to Report Witnessed Violations.* Failure to report violations you have witnessed may be interpreted as a willful violation of the policy of your own. Student employees may not aid another student employee in policy violations.
3. *Supervisors' Obligation to Report Violations.* Supervisors must report to the Dean of Students the nature of violations of this policy and the disciplinary action taken by the supervisor. The Dean of Students will counsel the supervisor on appropriate further action, if any.

#### **C. Discipline**

1. *Sanctions.* Violations of published information management policies may result in verbal reprimand and corrective counseling, written reprimand, or suspension/termination from University employment, at the discretion of the supervisor. The supervisor may take guidance from applicable statutes or other rules governing the information in question, as well as managerial judgment. Consultation with the Dean of Students is strongly encouraged (see B.3 above). In those cases wherein student conduct actions are anticipated, the student typically will be suspended from their University positions pending the outcome of the case in the student conduct system.
2. *Records.* Violations are entered on the student's conduct record, and are subject to conduct procedures managed by the Dean of Students. Violations may be subject also to civil penalties as dictated by relevant statute. Prior violations are also recorded in the student's file maintained by FAO, and will be taken into account in the process of application to work in other UNH offices.

#### **IV. Statement of Responsibility for Information Management**

I understand that through my employment at the University of New Haven I may have access to, or share responsibility for, confidential information, the improper disclosure of which may be prohibited by federal law, state law, and/or University policy. I understand that the willful mishandling of certain types of information could expose me to civil and criminal penalties, and could constitute just cause for immediate suspension or termination from employment by UNH and/or disciplinary action under the student conduct system.

If I am in doubt about proper procedures for the treatment of information, I will consult my staff/faculty supervisor for guidance prior to accessing or releasing the information.

My supervisor's signature below confirms their understanding of their responsibilities regarding my training and counseling to treat confidential information properly and to understand rules regarding access to offices, computers, files, and data systems that apply to my area.

My signature confirms that I have read and understood the statements above.

\_\_\_\_\_  
Signature of student employee                      date

\_\_\_\_\_  
Signature of staff/faculty supervisor                      date

---

This form must be submitted to the Financial Aid Office before a Work Authorization Card will be issued.