Approved By:	Cabinet
Effective Date:	January 5, 2009
Category:	General College
Contact:	Chief Information Officer (585) 245-5577

Confidential Information Policy

PROFILE

The State University of New York at Geneseo (SUNY Geneseo) is committed to protecting the privacy and confidentiality of information contained in the multiple databases and print files maintained by the College in the regular course of business. Personal information that is confidential in nature will be used only in accordance with the SUNY Geneseo Information Security Program, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) regulations, and all applicable SUNY, State and Federal regulations.

POLICY

Employees at the State University of New York at Geneseo (SUNY Geneseo) by nature of their positions will gain access to private personal information about students, faculty, staff, alumni, and other constituents of the College. Employees are obligated to maintain the confidentiality of any such private personal information that is encountered.

SUNY Geneseo expects all employees with access to personal information to deal with that information in a respectful and professional manner. As a matter of policy, the College restricts access to personal information to only those employees who have a legitimate "job-related reason" in the performance of their duties for gaining access. Access and release of any student educational records must be in accordance with FERPA regulations. Access and release of any health records must be in accordance with HIPAA regulations. Any personal information viewed or accessed by an employee through College systems or records is not to be shared or released to others unless there is a legally permissible purpose for doing so. In addition, in accordance with Section 203-d of the New York Labor Law, SUNY Geneseo will not:

- Publically post or display an employee's social security number;
- Visibly print a social security number on an identification badge, including any time card;
- Place social security numbers in files with open access; or
- Communicate an employee's personal "identifying information" to the general public.

Identifying information is defined to include an employee's social security number, home address or telephone number, personal email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number.

Inappropriate disclosure of information pertaining to students, faculty, staff and other college constituents may violate applicable law and regulations and is considered a violation of ethics and a breach of trust placed in employees by the College. Upon finding of a breach of this policy by an employee in a collective bargaining unit, the College may initiate disciplinary action pursuant to the applicable collective bargaining agreement, up to and including termination of employment.

For employees not covered by a collective bargaining agreement, sanctions may include actions up to, and including termination of employment.

Student employees who have violated these provisions will be referred to the student disciplinary process.

Volunteers who have violated these provisions will have their voluntary appointments terminated.

Employees who deal with confidential material on a regular basis will be required to sign a confidentiality statement. Each vice president, in conjunction with their managers, will determine employees required to sign confidentiality statements.

GUIDELINES

Employee, student, financial, and medical information contained within SUNY Geneseo information systems (electronic and physical files) and external SUNY systems is considered confidential. Access to information made confidential by law or campus practice is limited to those individuals (employees, consultants, adjunct professors, third-party vendors, etc.) whose position legitimately requires use of this information.

The employees (SUNY Geneseo faculty, staff, student employees, and volunteers appointed by the College) understand that by virtue of their work for SUNY Geneseo, they may have access to data that are confidential, and therefore understand they may not disclose such confidential data to any person or entity without appropriate authorization, subpoena, or court order.

Examples of such confidential information include, but are not limited to, the following:

- Social security numbers (SSN)
- Date of birth
- Motorist identification number
- Credit card numbers
- Bank account numbers
- Medical information
- Educational records
- Information (including directory information) made confidential by written request.
- Employee personal identifying information as defined in this policy.

In order to access confidential information, employees agree to adhere to the following guidelines:

1. Employees understand and acknowledge that improper or inappropriate use of data in the College's information systems is a violation of College policy, and it may also constitute a violation of federal and/or state laws.
2. Employees will not provide confidential information to any individual or entity without proper authorization.
3. Employees will not access, use, copy or otherwise disseminate information or data that is not relevant and necessary to perform their specific job-related duties.
4. Employees will not remove confidential information from College facilities except as specifically authorized to do so.

5. Employees will not share their user id and password with anyone, including support staff. Proxy access can be granted in some instances by request to the Office of the Chief Information Officer.

6. Employees will not use the data for personal or commercial purposes.

7. Employees will refer all requests for educational records from law enforcement governmental agencies and other external entities to the Dean of Students for matters related to students and to the FOIL Officer for all other requests.

8. Employees will refer external requests for all College statistical, academic or administrative data to the Office of Institutional Research, Office of Human Resources, or those departments that have been authorized to respond to such requests.

9. Employees will not communicate any SUNY Geneseo employee's personal identifying information to the general public.

10. Employees will report any unauthorized access to confidential data immediately to their supervisor and to the Chief Information Officer.

11. Employees understand that any improper or inappropriate use of data in the College's information systems may result in disciplinary action pursuant to the applicable collective bargaining agreement, up to and including termination of employment.

12. Employees are not permitted to store social security numbers, credit card numbers, motorist/non-driver ids or bank account numbers on individual staff computers, or portable media such as external hard drives, USB thumb drives, CDs, DVDs, tapes, etc. without express authorization from the Chief Information Officer. Storing other confidential data on individual staff computers or any type of portable media is strongly discouraged.

13. Employees storing confidential data on College servers must on an operational basis remove files containing confidential data when no longer needed.

14. Employees who are uncertain about what constitutes legitimate use or release of information should always err on the side of confidentiality and refer their questions about the appropriateness of a request for personal information from College systems or records to their supervisor before releasing the information.

PROCEDURES

1. Supervisors are required to review the Information Security Policy Regarding Confidential Information with each new employee assigned to their department. During the department orientation process, supervisors should provide each employee with a description of the type(s) of confidential information his/her specific position will work with in the performance of his/her duties.

2. Employees in areas of the College that deal with confidential material will be required to sign a confidentiality statement to be stored in the employee's personnel file. Each vice president in conjunction with their managers will determine employees required to sign confidentiality statements.

3. Supervisors shall review the policy on Information Security Policy Regarding Confidential Information on an annual basis and confirm in writing that each employee in the unit reviewed and understood the policy.