

CONFIDENTIALITY AGREEMENT

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 and its employees 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. 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.

As an employee or volunteer of SUNY Geneseo, I agree to abide by the following guidelines:

1. I 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 state laws.
2. I will not provide confidential information to any individual or entity without proper authorization.
3. I will not access, use, copy or otherwise disseminate information or data that is not relevant and necessary to perform my specific job-related duties.
4. I will not remove confidential information from College facilities except as specifically authorized to do so.
5. I will not share my 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. I will not use the data for personal or commercial purposes.
7. I 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. I 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. I will not communicate any SUNY Geneseo employee’s personal identifying information to the general public.
10. I will report any unauthorized access of confidential data immediately to my supervisor and to the Chief Information Officer.
11. I 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. I understand that I am 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. I understand that when storing confidential data on College servers, I must on an operational basis remove files containing confidential data when it is no longer needed.
14. I understand that if I am uncertain about what constitutes legitimate use or release of information I should always err on the side of confidentiality and refer my questions about the appropriateness of a request for personal information from College systems or records to my supervisor before releasing the information.

Printed Employee Name	Employee Signature	Date