| Title: **College Personnel Data Confidentiality Agreement** | Number: 200.106 |
|---|---|
| Section: General Administration/Computer | Created: 11/19/2012<br>Last Revised: 08/01/2013 |

College personnel by nature of their positions will gain access to confidential information (**CI**) about students, faculty, staff, alumni, and other constituents of the College. Personnel are obligated to maintain the confidentiality of any information that is encountered.

The College expects all personnel with access to CI to deal with that information in a respectful and professional manner. CI gained from employee or student records in the course of employment or function is not to be shared with anyone other than those authorized to receive the information. Electronic or hardcopy records are prohibited from leaving any office without approval from the office supervisor. Files will not be left unattended in areas where non-authorized persons could view them. Only authorized personnel are allowed in areas where confidential records are stored.

Access and release of any student records must be in accordance with FERPA regulations. Access and release of any Protected Health Information (PHI) 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 accordance with New York Labor Law, the College and its personnel 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 private information to the general public.

Inappropriate disclosure of information pertaining to students, faculty, staff and other college constituents may violate applicable law and regulations. Employee, student, financial, and medical information contained within the College's 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, volunteer, or other College workforce member with access to CI, I agree to abide by the following:

1. I understand and acknowledge that inappropriate use of data in the College's information systems is a violation of College policy and may also constitute a violation of federal or state laws.
2. I will not provide CI to any individual or entity without proper authorization.
3. I will not access, use, copy, or disseminate information or data that is not relevant to perform my duties.
4. I will not remove CI from College facilities except as specifically authorized to do so.
5. I will not share my assigned username and password with anyone, including support staff. Proxy access can be granted in some instances by request to the individual's supervisor and Director of Information Technology.
6. I will not use the College's data for personal or commercial purposes.
7. I will refer all requests for student records from law enforcement entities to the Registrar.
8. I will refer external requests for College statistical, academic or administrative data to the Office of Institutional Research and Planning, Public Relations, or those departments authorized to respond to such requests.
9. I will not communicate any College employee's personally identifiable information to the general public.
10. I will report any unauthorized access of CI immediately to my supervisor, who will inform the Vice President of Administration and the Dean of Information Technology.
11. I understand that inappropriate use of data in the College's information systems may result in disciplinary action pursuant to the applicable collective bargaining agreement, as the circumstances may warrant.
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, personal cloud-based storage or portable media such as external hard drives, USB thumb drives, CDs, DVDs, tapes, etc. without express authorization from the Data Owner as per Banner Data Standards. Storing other CI on staff computers or any type of portable media is strongly discouraged.
13. I will comply with the College's Bring Your Own Device (BYOD) and Mobile Device policy when accessing or storing CI on personal mobile computing/storage devices.
14. I will comply with the College's Records Retention and Disposition policy (available in the Business Office), as well as my departments' procedures for destroying of paper and data records.
15. I understand that if I am uncertain about what constitutes legitimate use or release of information, I should always refer my questions about the appropriateness of a request for CI to my supervisor before releasing the information.

| Signature: | Date: |
|---|---|