

BUFFALO STATE

Employee Guidelines for Securing Information

All personal and academic information is private and confidential and is protected by various state and federal laws. Buffalo State College employees must, by law, protect the privacy of this information.

Failure to protect personal and academic information may result in legal action against offending employees. Employees accused of failure to protect confidential information that results in harm to an individual may not be covered by Public Officer's Law, and therefore not defended by New York State.

Examples of personal information that must be kept confidential: Social Security numbers, health information, disability status, drivers license numbers, etc. Faculty and staff must ensure that information contained on the employee change form is kept confidential.

Examples of academic information that must be kept confidential: grades, student class schedules, student ID numbers, etc. Faculty and staff members may not post test scores or grades using any portion of a student's name, Social Security number, or student ID number. Faculty and staff must refrain from providing students' parents with information related to their student's academic performance or other personal information unless given permission to do so by the student.

Other information that must be protected includes procurement card information, vendor data, and donor information.

Ensure secure use of electronic resources

- Respect the privacy of other users: for example, users shall not intentionally seek information on, obtain copies of, or modify files or data belonging to other users unless explicit permission to do so has been obtained.
- Respect the legal protection provided to programs and data by copyright and license.
- Respect the integrity of computing systems: for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system or damage or alter the software components of a computer or computing system.
- Safeguard all accounts and passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person. Users are expected to report any observations of attempted security violations.

Manage e-mail messages and attachments appropriately

Because e-mail is a communication system, messages should not be retained for extended periods of time. If a user needs to retain information in an e-mail message for an extended period, the message should be transferred from the e-mail system to an appropriate electronic or other filing system.

Users should:

- Dispose of copies of records in e-mail after they have been filed in a record-keeping system.
- Delete records of transitory or little value that are not normally retained in record-keeping systems as evidence of college activity.

Control access to rooms and file cabinets where paper records are kept

- All doors to office areas must be locked during non-business hours.
- Work areas where customer information is processed must be behind locked doors or otherwise secured during business hours.
- Guests should be escorted in areas where customer information is being processed.
- Guests should be restricted to areas that do not have customer information in plain view. Conversely, customer information should be kept out of areas accessible to students and the public.
- File cabinets used to store customer information must be secured in locked areas.
- Fireproof cabinets used to store promissory notes must be locked during nonbusiness hours.
- Records containing customer information are to be retained only as long as they are valid, useful, and required to be retained. When no longer needed, paper, microfilm, and microfiche records must be destroyed by shredding. Electronic records must be destroyed according to current guidelines available from Computing and Technology Services. Retention guidelines are available from the Campus Services Office.

Control access to information stored electronically

- Workstations should be behind locked doors or otherwise secured.
- Employees should "minimize" any computer windows not in use, to prevent inadvertent breaches.
- Employees are encouraged to password-protect their workstations when not in use.
- Employees should use strong passwords for all systems (at least eight characters, alphanumeric).
- Employees should change their passwords every 60 days or less.
- Employees must not post passwords on or near their computers.
- Access to student and employee records systems will be granted only to those employees whose job duties require them to access customer information.
- Personal and academic information should be stored on a password-protected shared network drive. Sensitive information should not be e-mailed or stored on a laptop, desktop machine, or any portable storage device.
- Delete any sensitive files when they are no longer needed.
- Laptops and flash drives should be kept in a secure area to guard against theft of the devices and the information stored on them.
- Personal or academic information should not be removed from campus.
- Protect our customers' information:
 - Employees should respond to requests for customer information in accordance with the Family Educational Rights and Privacy Act (FERPA). FERPA questions or potential violations should be referred to the Registrar's Office.
 - Employees should refer to appropriate security policies as needed to ensure compliance.
 - Employees must report any fraudulent attempt to obtain customer information to management, who should then report the attempt to the Vice President for Finance and Management's Office.

For more information contact Tom Killian, Director, Networking and Operational Services (ext. 5122, killiatd@buffalostate.edu) or Judi Basinski, Associate VP, Computing and Technology Services (ext. 4206, basinsjb@buffalostate.edu).