BUFFALO STATE COLLEGE

DIRECTORY OF POLICY STATEMENTS

Policy Number:　　　VI:21:02　　　　　　　　　　　　　Date:　　January 2009

Subject:　　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. Examples of information that must be kept confidential: Social Security numbers, health information, disability status, grades, student class schedules, student ID numbers, drivers license numbers, procurement card information, vendor and donor data, etc.

PAY SPECIAL ATTENTION TO THE RISKS OF DISTRIBUTING SENSITIVE INFORMATION

- Sensitive information should not be e-mailed or stored on a laptop, desktop machine, or any portable storage device.
- Personal and academic information should be stored on a password-protected network drive (U:drive).
- 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.

SAFEGUARD STUDENT ACADEMIC INFORMATION

- Faculty members' grade book information should not be stored on laptops or other portable devices.
- 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 written permission to do so by the student.

SAFEGUARD YOUR CAMPUS ACCOUNTS

- Safeguard all accounts and passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person.
- Employees should use strong passwords for all systems (at least eight characters, alphanumeric) and change them frequently.
- Employees must not post passwords on or near their computers.
- Dispose of copies of records in e-mail after they have been filed in a record-keeping system.
- Delete e-mail messages of transitory or little value that are not normally retained in record-keeping systems as evidence of college activity.

CONTROL PHYSICAL ACCESS TO SENSITIVE INFORMATION

- Sensitive information should be kept out of areas accessible to students and the public.
- Control access to rooms and file cabinets where paper records are kept.

- 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.

For more information contact the Director of Networking and Operational Services or the Associate Vice President for Computing and Technology Services.