Overview

Bloomfield College regards security and confidentiality of data and information to be of major importance. Each individual granted access to electronic, verbal and/ or hard copy data must preserve the security and confidentiality of the information to which he or she is granted access. It is the policy of Bloomfield College that Confidential Information (defined below) may not be divulged, in any format, without approval by the President or a Vice President (or their designees). This includes Confidential Information processed on a typewriter, by hand, network server, micro or personal computer, electronic notebook or smartphone utilized in the College’s operations, email, and maintained in hard copy files or on electronic storage devices including but not limited to tape or disk devices. This policy will be strictly enforced. Non-compliance is a serious matter which may result in disciplinary action up to and including termination of employment.

Users of Confidential Information are required to abide by all applicable federal and state laws regarding confidentiality of data including, but not limited to, the Family and Education Rights and Privacy Act (FERPA), Gramm, Leach Bliley (GLB) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). All users of Confidential Information need to understand how these laws apply to the information that each person is accessing.

Please see the following links for more information:


All individuals with access to Colleague and other College computer systems need to read and abide by the College’s Acceptable Use policy found at:

http://www.bloomfield.edu/resources/helpdesk/acceptable-use-policy

Definition

Confidential Information is defined as:

- For students, faculty or staff: Any personally identifiable records, financial records (including social security and credit card numbers), student education records, including academic records
and disciplinary records except as permitted by law, health records, contracts, photographs, research data, alumni and donor records and personnel records.

- For the College: College financial data, computer or systems passwords, College issued systems log-ons and any proprietary data of the College.
- Other: Any other information for which disclosure is prohibited by federal, state or local laws.

**Duties of Individuals With Authorized Access to Confidential Information**

Any individual with authorized access to Confidential Information is given access solely for the business of the College and must not divulge that information outside of the College or to persons within the College not authorized to receive confidential information. Exceptions must be approved by the President or the Vice Presidents of the College. Individuals must:

- Access confidential information solely in order to perform his or her job responsibilities.
- Not seek personal benefit or permit others to benefit personally from any confidential information that has come to them from work assignments.
- Not make or permit unauthorized use of any confidential information in the College’s information systems or other records or remove information from the College.
- Not enter, change, delete or add data to any information system or files outside the scope of their job responsibilities.
- Not include or cause to be included in any record or report, a false, inaccurate or misleading entry.
- Not alter or delete or cause to be altered or deleted from any records, report or information system a true and correct entry.
- Not release confidential information other than what is required in completion of job responsibilities which is consistent with this policy verbally, in writing or electronically.
- Not exhibit or divulge the contents of any record, file or information system to any person unless it is necessary for the completion of their job responsibilities.

It is the individual’s responsibility to report any violations of this policy as outlined below.

All users of College information systems are supplied individual user accounts to access the data or systems necessary for the completion of their job responsibilities. Users of College information systems are required to follow the procedures outlined below.

1. All transactions processed by a user ID are the responsibility of the person to whom the user ID was assigned. The user’s ID and password must remain confidential and not be shared with anyone. Using someone else’s user ID is a violation of policy. To reduce the risk of a shared password you must remember not to post your password on or near your workstation. It is your responsibility to change your password immediately if you believe someone else has obtained it.
2. Access to any student or employee information (in any format) is to be based on specific job requirements. The appropriate Department Head and or Vice President is responsible for ensuring that access is granted only to authorized individuals. Written authorization must be granted for access to the various data systems of the College. Please use the data access form attached to this policy. Individuals are prohibited from viewing or accessing information, in any format, unless they are authorized to do so. Any access obtained without written authorization is considered unauthorized access. In order to prevent unauthorized use, the user shall log off all applications that provide access to confidential information, or lock their computer when leaving their workstation. Unless there is a specific business need, all workstations should be shut down at the end of the workday.

3. If you have any reason to believe that your logon and password have been compromised or revealed inadvertently, you should change your password and immediately notify your direct supervisor who in turn must notify the Department of Information Technology.

4. Upon termination or transfer of an employee, Human Resources will notify the Department of Information Technology regarding the termination of access to College computer systems. Department heads will terminate access to decentralized systems such as Donor Perfect and Hobsons.

5. Generally, students, temporary employees and consultants do not have access to the College records systems. Written approval by a Vice President or their designee is required to provide access to an individual in this group. These individuals will be held to the same standards as full time employees.

6. All logons to various College computer systems need to be assigned to a specific individual. “Generic” logons are not permitted.

7. All persons with access to confidential information agree to properly secure and dispose of any printouts or files that are created in a manner that fully protects confidential information.

8. If you suspect an information security breach has occurred or a violation of this policy, report such a violation to your direct supervisor and contact Information Technology immediately.

I understand that my access to confidential information is for the sole purpose of carrying out my job responsibilities and confidential information is not to be shared outside of the College and only to others who are authorized to have access to confidential information. Breach of confidentiality is subject to disciplinary action up to and including termination of employment.

Name: __________________________________________
Date: __________________________________________

Signature: ______________________________________
Bloomfield College
Application for Network, Voice and Data Access

Name:__________________________________________________________

Title:___________________________________________________________

New____ Change____

Department:_____________________________________________________

Building:_________________________Room:________________________

Phone Ext:_____________________________________________________

Applicant Signature:_________________________Date:________________

Requested Password for Network Access (must be at least 8 characters)  _______________
The system will force a password change upon first login.

Data Access Required:

Colleague (includes webadvisor) – applicant requires access to the following modules/mnemonics

_________________  ___________  ___________  ___________  ___________  ___________

_________________  ___________  ___________  ___________  ___________  ___________

ADP _______________________________________________________________

Cardsmith _________________________________________________________

Donor Perfect _____________________________________________________

Hobsons _________________________________________________________

Privatel _________________________________________________________
Blackboard__________________________________________________________
e2 to campus__________________________________________________________

Other (specify)________________________________________________________

Department Head/Chair or Vice President signature___________________________
Date:_________________

Forwarded completed form to Information Technology for Colleague, Network and Voice Access and a copy to administrator for other data systems. **Completed and signed data confidentiality policy acceptance needs to accompany this form.**

**IT USE ONLY**
Voice mailbox no _________________ Date Assigned_________________
Network log on _________________ Date Assigned_________________
E-mail login name _________________ Date Assigned_________________