ST. BONAVENTURE UNIVERSITY
CONFIDENTIALITY AGREEMENT

St. Bonaventure University makes every effort to abide by all applicable Federal and State regulations, guidelines, statutes and procedures pertaining to confidentiality and privacy, specifically:

• The Family Educational Rights and Privacy Act of 1974, as Amended (FERPA);

• The Health Information Portability and Accountability Act (HIPAA); and

• The Gramm-Leach-Bliley Act (GLB).

FERPA protects the privacy of student education records. HIPAA controls the release of Protected Health Information (PHI) dealing primarily with patient information. GLB safeguards customer financial information.

As a member of the St. Bonaventure University working/volunteer community, I understand that I may have access to student, employee or other individual academic, personnel, health and financial records that may contain individually identifiable information and that this information is considered confidential. Examples of private, confidential information include, but are not limited to: student academic information (grades, courses taken, schedules, test scores, advising records), educational services received, social security numbers, gender, ethnicity, citizenship, veteran and disability status, health records, financial information, financial aid applications, copies of tax returns, human resource records and passwords.

It is important to handle all confidential information with discretion and it should only be disclosed to others who have a need to know for legitimate business reasons. In most cases, data of an individually identifiable nature shall remain secure from public disclosure (release to third parties) without specific permission from the individual to whom the data applies, unless law allows disclosure without consent.

I acknowledge that I understand that improper disclosure of this information to any unauthorized person is prohibited under Federal law and could subject me to criminal and civil penalties imposed by law. I further acknowledge that any such willful or unauthorized disclosure also violates University policy and it will be cause for action by the University, whether it be removal from a volunteer assignment or disciplinary action up to and including termination from employment regardless of whether criminal or civil penalties are imposed.

Data originated or stored on University computer systems is University property. Only data that is required for one's job should be accessed. To safeguard computer data, I agree that I will not share my computer login information, will not leave my computer signed on when away from my desk and will change my computer passwords regularly.

I further agree to handle all confidential information with discretion, safeguarding it when in use, filing it in locked file cabinets when not in use, disposing of it properly (i.e. shredding) when no longer needed and not disclosing or discussing it with any unauthorized person while working/volunteering for St. Bonaventure University, or after my employment/assignment at the University **comes to an end**. Any University report or document shall not be shared with any third party without the specific and expressed permission from the Director or Department Manager.

I acknowledge I have read the full policy on the reverse of this document and understand that the most recent version can always be found at http://web.sbu.edu/friedsam/governing/

Individual Acknowledgement and Acceptance:

_____

Individual Name (Printed) Signature Date

Revised May 2018

Policy on Confidentiality of Data

Each employee, consultant, student, or person granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Users of University data and information are required to abide by all applicable Federal and State guidelines and University policies regarding confidentiality of data, including, but not limited to the Family Education Rights and Privacy Act (FERPA). All users of University data and information should read and understand how the FERPA policy, at https://studentprivacy.ed.gov , applies to their respective job functions. [Policies located within St. Bonaventure University Health Services cover the university's implementation of Health Insurance Portability and Accountability Act of 1996 (HIPAA).]

Any employee or person with authorized access to St. Bonaventure University's computer resources, information system, records, or files is given access to use the University's data or files solely for the business of the University. Specifically, individuals should:

a) Access data solely in order to perform their job responsibilities.
b) Not make or permit unauthorized use of any information in the University's information services or data.
c) Not enter, change, delete or add data to any information system or files outside of the scope of their job responsibilities.
d) Not include, or cause to be included in any record or report, a false, inaccurate or misleading entry.
e) Not alter, delete, or cause to be altered or deleted, a true and correct entry from any record, report or information system.
f) Not release University data other than that which is required in completion of job responsibilities.
g) Not exhibit or divulge the contents of any record, file or information system to any person except as it relates to the completion of job responsibilities.

In addition, individuals are not permitted to operate or request others to operate any University data equipment for personal business or to make unauthorized copies of University software or related documentation.

It is the employee/volunteer's responsibility to report immediately to his/her supervisor any violation of this policy or any other action, which violates confidentiality of data.

Procedures & Security Measures to Help Ensure Confidentiality of Data

All users of University information systems are supplied with a network account to access the data necessary for the completion of their job responsibilities. Users of the University information systems are required to follow the procedures outlined below:

1) All transactions processed by a user ID and password are the responsibility of the person to whom the user ID was assigned. The user's ID and password must remain confidential and must not be shared with anyone. Technology Services should be contacted in the event an administrative assistant requires access to a supervisor's account. Users should consider the following tips:

- Do not use anyone else's password. Using someone else's password is a violation of policy, no matter how it was obtained.
- Do not share your password with anyone. Your password provides access to information that has been granted specifically to you. Technology Services will never ask for your password. To reduce the risk of shared passwords – remember not to post your password on or near your workstation. Also, be sure that your computer is not set to automatically remember your password.
- Do not save your account password on any system so that it does not need to be entered manually.
- Do not respond to any requests for your password.
- 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 determined based on specific job requirements. The appropriate Director, Dean, Provost, and/or Vice President are responsible for ensuring that access is granted only to an authorized individual, based on the performance of his/her job. Technology Services must receive documented authorization prior to granting system access.

3) In order to prevent unauthorized use, users shall lock their computers when leaving the workstations, or shall establish an automatic screen saver to lock the computers, especially during breaks, lunch, and at the end of the workday. Users needing assistance with setting up these features should contact Technology Services.

4) Passwords should be changed if there is a reason to believe they have been compromised or revealed inadvertently. Users who suspect unauthorized use of a password should immediately notify their supervisors.

5) Upon termination or transfer of an employee, Human Resources will notify Technology Services. Technology Services will then take appropriate action to either terminate or modify the employee's computer access.

6) Generally, students and temporary employees should not have access to the University database (Datatel) system. Documented approval of the Director, Dean, Vice President or Provost in charge of the respective department is required if it is determined that access is required. Students, volunteers or temporary employees are to be held to the same standards as all University employees, and must be made aware of their responsibilities to protect student and employee privacy rights and data integrity.

7) Employees who are granted access to process transactions via Datatel have access to a secure information area. Any information entered or changed will be effective immediately. Employees are responsible for any changes made using their ID.