STUDENT RECORDS AND DISCLOSURES

FERPA

Family Educational Rights and Privacy Act (FERPA) Annual Notice to Students

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records. These rights include:

1. The right to inspect and review your education records within a reasonable time after Benedictine University receives a request for access. If you wish to review your record, contact the Office of the Registrar or the University office that maintains the record to make arrangements. You are required to submit your requests in writing and identify the record(s) you wish to inspect.
2. The right to request an amendment of your education record if you believe it is inaccurate, misleading, or otherwise in violation of your privacy rights under FERPA. If you feel there is an error in your record, you should submit a statement to the University official responsible for the record, clearly identifying the part of the record you want changed and why you believe it is inaccurate or misleading. That office will notify you of their decision and advise you regarding appropriate steps if you do not agree with the decision.
3. The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent. One exception which permits disclosure without consent is disclosure to school officials with legitimate educational interests. This includes any University faculty or staff employee (including the Benedictine University Campus Safety) acting within the scope of his or her University employment and with appropriate supervisory authority; any individual or entity with whom the University has contracted as its agent to provide a service to the University when acting within the scope of the contract or agency and who is subject to appropriate confidentiality requirements; any member of the University's Board of Trustees; any student serving on an official committee, such as a disciplinary or grievance committee; and any student assisting a University official in performing tasks for which the University official may have access. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities. Benedictine also discloses education records without consent to officials of another school in which a student seeks or intends to enroll or has previously enrolled such as through partnerships and consortium agreements.
4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the University to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:
   Family Policy Compliance Office
   U.S. Department of Education
   400 Maryland Avenue, SW
   Washington, DC 20202-5901

FERPA permits the release of directory information to third parties outside the institution without written consent of the student, provided that the student has been given the opportunity to withhold such disclosure. Benedictine University defines directory information as follows:

- Student's name, address, and phone number
- Major, minor, concentration, emphasis, specialization, and other fields of study
- Participation in officially recognized activities and sports
- Dates of attendance
- Degrees and awards received
- Most recent education institution attended
- Full-time/part-time enrollment status
- Photo
- Height, weight, and GPA of student athletes

A student may withhold disclosure of their directory information by completing the "FERPA Non-Disclosure of Designated Directory Information (https://ben.edu/wp-content/uploads/2022/08/FERPA-Non-disclosure-of-Designated-Directory-Information-Updated-6-15-17.pdf)" form available in the Office of the Registrar, within ten (10) calendar days of the first scheduled class day of each fall term. A request to withhold disclosure of directory information is effective for one academic year only and must be renewed each year.

In compliance with the Solomon Amendment, directory information is provided to the United States Department of Defense, upon request.

A student may authorize the release of confidential information (including personally identifiable information from education records protected by FERPA, and other types of confidential information as well) to a third party by signing an Authorization for Release of Confidential Information to a Third Party form (https://ben.edu/wp-content/uploads/2022/08/FERPA-Form-Confidential-Release-of-INformation-to-Third-Party.pdf).

The University may also disclose student account and financial aid information without the student's consent to the student's parents if the parent requests the information in writing; completes the Parent Certification section of the Authorization For Release of Confidential Information to Parents (https://ben.edu/wp-content/uploads/2022/08/FERPA-Confidential-Release-of-Information-to-Parents-Updated-09-02-2021-DKC-1.pdf); and provides evidence that the student is his or her dependent for federal income tax purposes. The University may also disclose information to a parent if there is a health or safety emergency involving their son or daughter, or if their son or daughter is under the age of 21 and has violated a federal, state or local law or any University rule or policy concerning the use or possession of alcohol or a controlled substance.

FERPA permits the disclosure of students' education records, without consent of the student, if the disclosure meets certain conditions of the FERPA regulations. Benedictine University may disclose from the education records without obtaining prior written consent of the student the following:

- To other school officials, including instructors, within Benedictine University who are determined to have legitimate educational interests. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities. Legitimate educational interests include performing a task or engaging in an activity related to one's regular duties or professional responsibilities, a student's education, the discipline of a student, a service to or benefit for a student, measures to support student success, evaluation of academic programs, and

the safety and security of the University. Individuals at the institution who have an educational interest in the student's educational record may share information internally to school officials that have a legitimate educational interest. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced services or functions.

- To officials of another school where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer.
- To authorized representatives of the U.S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the Illinois Board of Higher Education or other state agencies responsible for supervising Benedictine's education programs. Disclosures may be made in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of student records to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf.
- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid.
- To organizations conducting studies for, or on behalf of, the school, in order to:
  a. develop, validate, or administer predictive tests;
  b. administer student aid programs; or
  c. improve instruction.
- To accrediting organizations to carry out their accrediting functions.
- To comply with a judicial order or lawfully issued subpoena.
- To appropriate officials in connection with a health or safety emergency.
- To the general public, the final results of a disciplinary proceeding, if Benedictine University determines the student is an alleged perpetrator of a crime of violence or non-forcible sex offense and the student has committed a violation of the Benedictine University rules or policies with respect to the allegation made against him or her.
- Upon written request, the University will disclose, to the alleged victim of a crime of violence or a non-forcible sex offense, or to the alleged victim's next of kin (if the victim dies as a result of the crime or offense), the final results of any institutional disciplinary proceeding dealing with that crime or offense.

University Promotional Photos/Videos

Benedictine University and its representatives on occasion take photographs/videos for the University's use in print and electronic media. This serves as public notice of the University's intent to do so and as a release to the University giving permission to use such images as it deems fit. If you should object to the use of your photograph, you have the right to withhold its release by contacting Marketing and Communications at: https://ben.edu/marketing-comms/.

Student Right-To-Know Act

The University provides data on retention and graduation rates through the Office of Institutional Research and at the University Information (https://ben.edu/compliance-and-risk-management/) web page.

Information on financial assistance, including descriptions of application procedures and forms, may be obtained from the Office of Financial Aid (https://www.ben.edu/financial-aid/) on the Lisle Campus (Goodwin Hall). Information concerning athletic program participation may be obtained from the Athletics Department (https://benueagles.com/sports/2016/7/20/compliance.aspx) on the Lisle Campus (Rice Center) and Athletics Department (https://ben.edu/mesa/athletics/) on the Mesa Campus. Other institutional information including: the cost of attendance, accreditation and academic program data, facilities and services available to disabled students, and withdrawal and refund policies are located elsewhere in this Catalog.

Campus Security Policy and Campus Crime Statistics Act

Benedictine University's Annual Security Report and Annual Fire Safety Report are available online. These reports meet the requirements of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act for the reporting of crime statistics, fire safety information, and other relevant University policies. The electronic versions of these reports are available on the Benedictine University website at:

Campus

Annual Security and Annual Fire Safety Reports
https://ben.edu/campus-links/campus-safety/campus-safety-reporting/
Printed copies of these reports may be obtained at:

- For Lisle: the Benedictine University Campus Safety (ground floor of the parking structure located in the southwest part of the Lisle campus) or by calling the non-emergency telephone number, Lisle (630) 829-6122.
- For Mesa: the Benedictine University Campus Safety (Gillett Hall) or by calling the non-emergency telephone number (602) 888-5516.

Acceptable Use of Technology

Purpose

To help foster and protect the technology environment for the promotion of teaching, learning, research, business, and service, Benedictine University requires all users of its technology resources to comply with standards of academic and professional ethics, University codes of conduct and policies, and all applicable laws and regulations.

This policy details the University's ownership and monitoring of its Technology Resources, as well as the requirements for obtaining access to, and proper usage of those resources by Authorized Users. This policy applies to all persons and all devices accessing or using any Benedictine University information system or service.

Definitions

1. Authorized Users: Students, faculty, staff, emeriti, invited guests, contractors, agents, and all other persons granted authorized access or user privilege.
2. University IT Resources: University owned, operated, leased, licensed, or contracted networks, telephones, systems, and services, whether local or hosted, individually controlled or shared, including:
   - Wired and wireless networks
   - Student and staff information systems and databases
   - University provided email accounts and services
   - Networked and local storage systems and devices
   - Telephone and other communication systems

- Accounts operated by the University, including social media and other hosted platforms
- University data maintained in electronic format

In addition to this policy, users of University IT Resources agree to abide by the rules and regulations contained in applicable guidelines and policy and procedure manuals, as well as state and federal laws, including but not limited to those dealing with:

- FERPA
- HIPAA
- GLBA copyright infringement
- Defamation
- Discrimination
- Fraud
- Harassment
- Identity theft

Policy

Benedictine University recognizes that free expression of ideas is central to the academic environment. For this environment to flourish, all users must adhere to this policy.

Benedictine University voluntarily provides technological resources. The primary purposes of these resources are to meet the academic, research, administrative, and communications needs of its students, faculty, and staff. The use of these resources for other purposes is tolerated provided that usage is kept to a minimum and does not violate

1. any federal, state, or local law,
2. the University mission or policies, and
3. guidelines or rules stipulated in this policy.

Users who make incidental personal use of University Technology Resources do so at their own risk. The university cannot guarantee the security or continued operation of any Technology Resource.

Access to any Benedictine University owned and/or operated technology resource is a privilege and not a right. Individuals who refuse to follow the Acceptable Use Policy will not be granted user accounts or may not be granted access to services/systems. Violations of this policy by individuals with accounts may result in penalties including but not limited to closure of all accounts and revocation of all privileges. Other penalties may be levied up to and including dismissal from the University or termination of employment.

Confidential Data

All users are to utilize all appropriate precautions to maintain the accuracy, integrity, and confidentiality of confidential data and ensure that no unauthorized disclosures occur. All users must refrain from sharing confidential data with anyone not authorized to view or possess such data. All users must comply with the provisions of the Benedictine University Confidentiality Agreement and all federal/state/local privacy laws and regulations, including GLBA and FERPA.

University Ownership/ Monitoring

Technology Resources are the property of the University. The University's ownership of a file, record, data or a message does not transfer ownership to the University of any intellectual property therein. Incidental personal uses are permitted as provided in this policy and are included in the definition of Technology Resources for the purposes of University access and use. Records of electronic communications pertaining to the business of the University are considered Technology Resources.

The Provost or the cognizant Vice President may grant access to the account of an Authorized User to other University employees or designated individuals when specifically authorized in writing, as long as the request includes the following:

1. What access/user account is being requested?
2. Why is this being requested? and
3. Who is going to access this information and for what duration?

The University President, Chief of Staff and Counselor to the President, General Counsel, or Chief Information Officer may also provide written authorization to grant access following the procedure set forth herein.

Expectation of Privacy

All technology resources, including email accounts and shared storage, are provided by Benedictine University in furtherance of its mission. No representation has been made to Users as to the privacy of any communication or data stored on or sent through Benedictine University technology resources. Users should have no expectation of privacy while using the University network or any technology resource. Email and files that are sent, received, or stored using University resources are the property of the University. Email is not a secure form of transmission. Benedictine University reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of University rules or policies. Benedictine University also reserves the right periodically to examine any system and any other rights necessary to protect its computing facilities.

The University may monitor the activity and accounts of Users of Technology Resources, with or without notice, when:

1. The user has voluntarily made them accessible to the public, as by posting to a blog or a web page;
2. It is necessary to protect the integrity, security, or functionality of University or other Technology Resources, or to protect the University from liability;
3. There is reasonable cause to believe that the user has violated, or is violating, this Acceptable Use Policy, or other University policies or guidelines, or laws or regulations;
4. An account appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns; or
5. It is otherwise required or permitted by law.

Any such monitoring, other than of information made available voluntarily or necessary to respond to emergency situations, must be authorized in advance by the University President or the University's Legal Counsel after consultation with the University President. If such monitoring is of the University President, then it must be authorized in advance by the University's Legal Counsel.

The University, in its discretion, may also disclose the results of such monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies, and may use those results in appropriate University disciplinary proceedings.

Under certain circumstances, the University may access and modify the contents of an email account. In cases concerning the health,

safety or welfare of the University community, as determined by senior University officials, the University may authorize accessing or modifying an employee's email account. In cases where personally# identifiable information may have been inappropriately disclosed, University officials may authorize modification of the email accounts of both senders and recipients.

The Benedictine University computing and Technology Resources constitute a private system. As such, the information stored on University owned or contracted equipment is the property of the University with the exceptions noted in the Creative Works section of the Faculty Handbook.

The University may use software tools to block electronic content and shape network bandwidth. These tools, such as Anti#Spam, Anti#Virus, and Firewalls, will be used to ensure the security of the technology environment. Web sites and Internet services may be blocked if they are known to spread viruses, spyware, adware, or other types of malicious software or service, harm or attempt to harm any University Technology Resource, or illegally host copyrighted material made available for download.

User Responsibilities

Users are responsible for all activity that happens on their accounts.

All users must:

- Maintain the privacy and security of all data;
- Keep passwords confidential;
- Comply with all information security policies and procedures;
- Be responsible for the data stored on his or her system, or in a shared network drive, by ensuring backups are maintained and controlling access, when appropriate;
- Adhere to all laws and regulations regarding copyright and intellectual property;
- Report any security incident or suspected misuse of any technology resource to the Chief Information Officer or designate.

All users must not:

- Install software or use any computing device in any way that degrades the network or makes inaccessible any other technology resource for any user;
- Share passwords with anyone or otherwise grant access to another person (except IT personnel) to their own account, computer, or other resource provided by the University;
- Obtain extra electronic resources or access to accounts for which they are not authorized;
- Misuse, alter, or otherwise damage any computer equipment;
- Engage in any activity designed to spy on network traffic or to access other users' accounts, passwords, files, or programs;
- Display or cause to display pornographic, obscene, abusive, racist or inappropriate material at any public or employee workstation or digital display. The University reserves the right to judge the appropriateness of displayed material;
- Install unlicensed or "pirated" software;
- Install software on a student#accessible computer (with the exception of Information Technology staff);
- Use University technology resources to relay mail;
- Install network or other technology hardware (including wireless access points, hubs, switches, etc.) without prior written authorization from the Chief Information Officer. Unauthorized equipment will be confiscated;
- Use any technology resource to support political or non#University related business interests;
- Represent the University on social media or by any technology means unless authorized to do so
- Disable, remove, or uninstall software designed to provide a secure computing environment, including patches of existing software, on any institutional information system without prior approval from IT.
- Sell, rent, or provide access to University technology resources to outside individuals, groups, or businesses except as authorized by the Chief Information Officer for authorized University business relationships

Enforcement

Benedictine University retains unfettered discretion to monitor, authorize, control or stop the use of said technology at its sole discretion. Alleged violations of the Acceptable Use of Policy will be referred to the Vice President of Student Life (students), the Provost (faculty), or the Vice President for Administration and Finance and Chief Financial Officer (non#faculty employees) for investigation and action through the established disciplinary processes of the University. Violations of this policy may result in disciplinary action up to and including expulsion or separation from the University, and may also result in legal action. In addition, the University may:

- Delete files or programs;
- Inactivate user access privileges;
- Remove the user account.

If a user believes that her or his rights have been violated by another user of University technology resources, the user should report the incident to the Vice President of Student Life (students), or her or his supervisor (faculty and staff) for appropriate action.