



Guide to Information Security for Faculty and Staff

University of Massachusetts Boston

Office of the Registrar

<http://www.umb.edu/registrar>

Information Technology

<http://www.umb.edu/it>

*With special thanks to the Office of
Information Technology, University
of Massachusetts Amherst, for
graciously allowing us to adapt their document.*

Guide to Information Security for Faculty and Staff

Use this guide to find how to handle sensitive student information securely and what steps you can take to protect your office and computer environment against potential security breaches.

1. Student Information at UMass Boston

What is FERPA anyway? 3

Directory Information 4

Photos & ID Numbers 5

Academic Records 7

2. Storing Student Information

Do I really need to save this information? 10

Secure Your Computer 11

Restrict Access to Your Data. 14

3. Sharing Student Information

Email & Instant Messaging (IM) 17

Learning Objectives

By the end of this section, you will know:

- What qualifies as public versus confidential student information at UMass Boston
- What constitutes a FERPA violation
- What you can do to avoid breaking the law

Section One: Student Information at UMass Boston

Use this section to learn more about the Family Educational Rights and Privacy Act of 1974 (FERPA) and its relevance in instructional contexts.

What is FERPA anyway?

FERPA (the Family Educational Rights and Privacy Act) is a federal law that protects the confidentiality of student records.

At UMass Boston, most student information is *confidential*, and cannot be made public without the student's consent. The FERPA confidentiality requirements apply to all current and former students, starting when a student matriculates.

Note: These confidentiality requirements are based on the University's official interpretation of the FERPA law and other relevant state laws. FERPA may be interpreted and applied differently at other institutions.

FERPA Violations

FERPA violations can have serious repercussions for you, your students, and the University. In addition to legal consequences, (accidentally) releasing FERPA-protected information may also compromise students' safety. Making your class roster public, for example, confirms a student's schedule and can help locate the student on campus. This is a serious issue, especially for those students who restrict access to their information for personal safety reasons, such as stalking and harassment.

Assume all student information is confidential

Although portions of a student's record are public (see directory information below), we recommend that you treat all student information as if it were confidential. This means declining to give out any student information to anyone (including parents) and referring any information requests to the Registrar's Office.

Directory Information

Typically public, unless the student has a "privacy flag."

Personal & Contact Details

- Name
- Place of birth
- Weight & height
(members of athletic teams only)

Academic Details

- Dates of attendance at UMass
- Major
- Participation in officially-recognized University activities and sports
- Degrees, certificates and awards
- Student employment status
- Most recent previous educational institution or agency attended

Directory Information

Students' directory information is typically public

Under FERPA directory information may be made public. The data elements that may be made public at UMass Boston are listed in the sidebar.

Students can request that their directory information be kept private

To withhold access to their directory information from any third party, students may fill out a confidentiality form, available at the One Stop, Upper Level, Campus Center.

To find out whether a student has submitted the confidentiality form, check with the support staff in your department. If a student has submitted the form, a "window shade" privacy icon



will appear on each page of his/her record in the student administration system, but not in WISER Faculty Self Service.

Directory Information in the Classroom

Privacy flags apply to the outside world, but not within the classroom

Students can expect their directory information to be protected from the outside world, but not from other students in the same class. This means that it is acceptable for instructors to use:

- Attendance sheets with students' names
- Email lists with students' email addresses

Students' enrollment in your class is always confidential

Students' names may be public, but their class schedule is not. You cannot publicly link students' names with your class without their consent since this confirms part of their class schedule and may help locate them on campus.

Honor your students' privacy requests

Although FERPA does not protect the directory information of students taking the same class (even for those students who request a full privacy flag), it is



FERPA Violations

- Leaving attendance sheets that identify your class and your students in a public place.
- Confirming a student's enrollment in your class to anyone, including the student's parents, spouse or employer.

always a good idea to keep this information confidential when your students specifically request it.

What is Blackboard Learn?

Blackboard Learn is the learning management system (LMS) for on-line courses and courses that have an on-line component. It offers tools for the development, delivery, and administration of course materials online.

Because students have to log in with their campus email address and can only access courses for which they are registered, Blackboard Learn can be considered an extension of the classroom for FERPA purposes.

This means that activities that are acceptable in the classroom (e.g., circulating an attendance sheet) are also acceptable in Blackboard Learn.

Photos & ID Numbers

Students' photos and 8-digit student IDs are always confidential. No exceptions.

Do not use UMass Boston Student IDs (or a portion of these IDs) to identify students on public grade lists and exam score sheets

Grades and exam scores can be posted in public only if they are not ordered alphabetically and they do not contain any personal information. If you usually post exam scores on your office door or upload grades to your public course Web site, consider assigning a random number to each student at the beginning of the semester.

Do not post class photos in public online spaces where anyone with an Internet connection can identify your students. You may upload class photos only to online services that allow you to restrict access to your materials (e.g., Blackboard Learn, a password-protected Web site, etc.).



FERPA Violations

- Posting a class photo on your public blog or course Web site.
- Using a portion of students' UMass IDs on the exam score list posted on your office door.

Identity Management in the Classroom: Give Students Control over their Information

Avoid breaking the law by letting your students control the information they share with the class and the outside world.

Alert students about the public nature of certain instructional technologies (e.g., blogs, wikis, public course Web sites, social bookmarking services). Students concerned about their privacy can choose user names that do not identify them by their real name and explore any built-in privacy options (if available).

Make group photos optional

If you plan on uploading a class photo to a public online space, allow your students to “opt in” and do not penalize them if they choose not to participate.

Students' Academic Records

The following are confidential and may not be shared with others without the students' explicit permission.

Class materials (any materials for which students receive a grade)

- Class assignments: exams, research papers, reports, art projects, experiment results
- Supplementary materials: discussion posts, blog entries, assignment drafts

Grades, exam scores, and any related information that indicates a student's progress in a class.

Instructor's evaluation of a student's work: feedback, comments, or suggestions delivered in any format (formal/informal) and via any medium (in person, on paper, or on the Web).

Academic Records

Students' academic records are always confidential

To share academic records information with others, you need the student's consent first.

Academic records are not limited to students' grades

In instructional contexts, academic records also include assignments and the instructor's feedback on students' class work.

Academic Records in the Classroom

Do not post grade lists in public

Students can access their own grades in WISER Student Self Service. Under FERPA, you can make grade lists public only if the list is scrambled (i.e., not alphabetical) and it does not identify students by any personal information.

Do not leave graded assignments in public areas

A common practice is to leave final assignments in departmental mailrooms or outside office doors for students to pick up at the end of the semester. This compromises confidentiality since it enables students to see their peers' grades and makes grade information publicly available.

We recommend that you leave graded projects in individual envelopes with the support staff in your department. These staff members can check students' ID cards before handing out their assignments.

Keep your feedback private

Communicate your feedback to students directly, via email or in person; avoid public online spaces where comments are available to anyone (e.g., blogs, wikis, Flickr, etc.).

Legitimate Educational Interest

FERPA requires that faculty and staff have a “legitimate educational interest” in order to access or make students’ records public without their prior consent.

The term has a broad legal definition that includes acting in the student’s educational interest and an employee’s need to fulfill job-related responsibilities.

At UMass Boston, ‘legitimate educational interest’ refers to “academic status check or evaluations, research, curriculum evaluation or development, institutional/statistical evaluation and analysis, student placement, public safety, and admissions evaluations.”
(Academic Regulations)

Exceptions based on “legitimate educational interest”

In classes where students and instructors assess individual projects as a group (e.g., speeches, art projects), the instructor’s feedback is often public. This is not considered a FERPA violation as long as these critiques are necessary for students’ learning (i.e., they serve a “legitimate educational interest”).

If you are teaching a class that involves collective feedback, make sure:

- Your syllabus briefly describes these sessions
- Your feedback does not mention a student’s grade in public
- The contents of these sessions are not available to the outside world

FERPA & Advising

Obtain the Student’s Consent First

Parents often contact advisors about students’ academic progress.

Before you reveal any information to a parent, we recommend that you have a release form with the student’s signature on file.

Students can request access to their advising record

Under FERPA, students have the right to review their personal and academic records. The University is required to provide students with copies of their records and consider requests to amend any inaccurate information that these records may contain.

Your advising notes are part of a student’s academic record and can be reviewed any time. It is important that you keep them factual (support your recommendations with concrete information) and explicit (are your abbreviations intuitive enough?). Don’t forget to date your comments!



FERPA Violations

- Telling a student’s mother that she is failing your class.
- Posting evaluations of your students’ projects in a public online space (e.g., wiki, blog, Web site, etc.)
- Leaving graded assignments in your department’s mailroom at the end of the semester.

FERPA Questions?

Registrar's Office (617-287-6200)

***Publicizing Students' Class Work:
FERPA vs. Copyright***

If your conference presentation or research paper uses work that students developed in your classes, and you are crediting these students by name, FERPA requires that you obtain the students' consent before publicizing their work.

This principle applies to any medium in which student work is showcased (e.g., at conferences, in journal articles, on departmental Web sites, in brochures and other print materials, etc.). In this context, "student work" refers to any material developed as part of a class for which students were evaluated (e.g., reports, drawings, discussion posts, etc.).

The FERPA & Copyright Catch-22

It is a FERPA violation to publicly link students' names with class work for which they were graded without their consent.

It is a copyright violation to use students' class work without crediting them by name.

Learning Objectives

By the end of this section, you will know how to:

- Choose a safe storage location for confidential information
- Protect your computer against security breaches
- Restrict access to sensitive data

Section Two: Storing Student Information

Use this section to learn how to store (student) information securely. Find out more about our preferred storage options and what you can do to maintain a secure information environment.

Do I really need to save this information?

This should be your first question *before* storing any FERPA-protected information in your office or on your computer.

Do not save any student information unless absolutely necessary. If you need to save student information (e.g., transcripts, assignments, grade lists), please remember:

Guidelines for Saving Digital Files

Not all storage options are created equal

Use caution when saving confidential documents on laptops, portable storage devices (e.g., CDs, USB drives), or shared computers. If you choose one of these storage options, consider using passwords or encryption as an extra security layer. For assistance with encryption, contact the IT Service Desk (617-287-5220).

Protect your software and hardware

Make sure that you routinely use anti-virus software and that your operating system is updated with the latest security patches and updates. Do you always keep your hardware in a secure physical location?

Use OneDrive to store confidential files, including your students' assignments, projects, and grades, or your own personal records. Access your Onedriveiles from on or off-campus, from any computer with an Internet connection.

What is OneDrive?

OneDrive IT's Web-based file storage and sharing system, provides a secure storage alternative for sensitive information.

We recommend storing FERPA-protected documents on OneDrive because:

- **They're safe.** Onedrive uses the appropriate security protocols to protect your files.
- **They can't get lost.** OneDrives gives you the flexibility of a portable storage device without the "easy-to-lose" factor. No need to worry about losing or misplacing a disk or drive.

Learn more about OneDrive from https://www.umb.edu/it/admin_systems/onedrive

Guidelines for Saving Paper Documents

Choose a safe location (e.g., a locked drawer)

Do not leave copies of confidential documents on your desk or in your classroom.

Shred any copies you no longer need and are not considered part of the student's academic record.

Recycling without shredding is not a good idea in this case.

Protect your Mac!

Macs play a critical role in a secure information environment. Did you know? Even if not infected, Macs can help transmit viruses to Windows computers.

Don't take your Mac for granted!

- **Use your anti-virus software.** Run a full scan of your computer at least once a semester. Configure your anti-virus application for automatic scans and updates.

<http://www.umb.edu/it>

- **Stay informed.** Check the IT web site and the Apple web site for the latest security news and advisories.

Secure Your Computer

Security breaches occur most often on computers that are not up-to-date and that do not use the most recent anti-virus software. The most important steps you can take to secure your computer are to use anti-virus software and to keep your operating system updated.

Install Protective Software

Viruses and other malicious software can infiltrate your machine and perform unwanted tasks, compromising your documents and computer programs.

Install the appropriate version of anti-virus software for your computer

Anti-virus software is available to members of the University community at no charge. Contact the IT Service Desk (itservicedesk@umb.edu) for assistance.

Update your virus definitions

Keeping your virus definitions updated ensures that your anti-virus software recognizes new forms of malicious software and detects new virus strains.

Enable automatic scans and on-access scanning

Automatic scans help you to routinely monitor your computer for any suspicious activity. On-access scanning provides continuous scanning and virus detection when new files are opened or

saved to your computer.

Note: In addition to automatic and on-access scans, we recommend that you run a full scan of your computer at least once a semester.

Keep Your Software and Operating System Updated

Security breaches occur most often on systems that are not up-to-date. It is critical that you:

Install security patches

Software vendors routinely release patches and fixes that cover known vulnerabilities and security holes. Protect your computer by keeping it updated with the latest patches, updates, and drivers.

Enable automatic updates

By enabling automatic updates, your computer will receive critical patches every time you connect to the Internet.

Contact the IT Service Desk for help in setting up automatic updates.

Protect Your Computer against Malware

Watch out for malware (a.k.a. spyware and adware). Malware is a generic term for various types of malicious software, known for corrupting Windows operating systems, causing conflicts with legitimate software, and leaving your computer vulnerable to worms and other viruses. Malware is also known for hijacking personal information and relaying it to advertisers and other third parties.

Use spyware detection programs

Use McAfee VirusScan, which comes with a built-in spyware detection and removal feature, or other reputable software (e.g., Ad-Aware, SpyBot Search & Destroy).

Download software only from reputable sources

Be particularly suspicious of “personalized offers,”

“scare tactics” and software that claims to speed up your Internet connection.

Restrict pop-up ads

Some malware infiltrates your computer via random pop-up windows. Allow pop-ups only for trusted sites like WISER. By enabling your browser’s pop-up blocker, you win twice: you avoid aggressive online advertising and protect your computer against malicious software!

Protect Your Hardware

These are basic safety rules, but how many times have you wondered whether you locked your office door?

Lock away your CDs, USB drives and any other storage media

Use a laptop security cable to lock your laptop to your desk. Most computer retailers have them available at accessible prices.

If your office has a door, lock it at the end of the day!



FERPA Violation

Sharing your campus email user ID and password.

By sharing your logon information, you put your students' information at risk. You will lose your access if the Registrar's Office detects any FERPA violations associated with your user ID.

If you absolutely must write down your password....

- **Write down password hints**, not the actual passwords.
- **Keep your ID and password information separate**: do not save user names and passwords in the same place.
- **Consider password storage software** that keeps all your passwords in one central location

(Mac OS X)

Enable the key chain feature (be careful, if you forget your master password, all your passwords will be unrecoverable).

(Windows)

Consider a commercial product similar to the key chain component for Macs.

Restrict Access to Your Data

Use Strong Passwords

Passwords are the weakest link in maintaining your computer's security. It is critical that you

Choose strong passwords

Password-guessing software often uses "dictionary attacks" (i.e., trying every combination of characters) to break passwords. Your passwords should always include letters, numbers, and characters. Never use full words or personal information.

Change your passwords on a regular basis

To guard against "dictionary attacks", you are required to change your campus email password every six months. Consider changing your other passwords at the same time.

Always say "No" when prompted to save a password

Some browsers offer to save your passwords. Get in the habit of always saying "No".

Do not recycle passwords

No matter how tempting, do not use the same password for different accounts. It's bad if your email is hacked. It's even worse if your mail *and* bank account are broken into.

Do not write down passwords

Storing your passwords on a post-it note on your monitor is an open invitation to access your computer. We believe that no location is safe enough for storing passwords.

Do not share your passwords

It is a violation of UMass Boston policy to share your password. By making passwords available to others (even people you trust), you put your personal information at risk and make it vulnerable to misuse.

Password-protect Your Files

Use passwords to "lock" individual documents

Passwords allow you to add an extra layer of security to files that contain sensitive information.

Consider assigning passwords to all documents containing student information that you store on disks, thumb drives, and other portable storage devices.

Set up User Accounts

Users who log in as “Administrators” for every computer session put their computers at risk because viruses are most harmful when they enter via an Administrator Account. We recommend that you create a User Account for everyday use and save Administrator access for administrator-level tasks such as software installation. Contact the IT Service Desk (itservicedesk@umb.edu) for assistance in setting up a user account on your computer.

User accounts should always be used on shared computers. This ensures that any student information you may have saved on your machine remains confidential and is not accessible to others.

Use Password-protected Screen Savers

Once you have enabled a user account, you can restrict access to your computer when you step away from your desk. Password-protected screen savers allow you to lock your computer temporarily without shutting it down. The screen saver will prompt you for your user account password once you are ready to resume your work.

“Sanitize” Old Computers and Media

Before you sell, recycle, or get rid of your computer, sanitize it first - make sure your hard drive is completely erased (wiped) and its contents are permanently removed.

Tossing your files in the ‘Recycle Bin’ is not enough

Placing files into the computer’s trash and then emptying the trash deletes only the visible portion of these files. Their contents are still retrievable

using readily available data recovery software.

Stay current with the UMass Data and Computing Policies Data purging is required when disposing of any University-owned electronic media. Disposal refers to recycling, salvaging or transferring ownership of computer and other technical equipment.

Learn more from:

<https://www.umassp.edu/bot/policies>

Data Purging

For assistance in purging a hard drive, send a message to itservicedesk@umb.edu or call 617-287-5220.

Learning Objective

By the end of this section, you will know the dos and don'ts of sharing student information securely.

Section Three: Sharing Student Information

Use this section to learn more about sharing (student) information securely. Find out more about our preferred communication tools and what you can do to avoid a security breach

Email & Instant Messaging (IM)

Use 2H0YH

□ sharing capabilities make it a convenient alternative to sending email attachments. Keeping the data file on your 2QLYHspace and controlling access to it is better than sending out attachments that may get forwarded or stored in insecure locations.

Use 2QLYHr:

- Collecting grades from your Teaching Assistants
- Providing feedback to your students
- Receiving and returning assignments

Use Your Campus (Encrypted) Email Account

Not all email services are created equal

The security protocols used to protect your information often vary by email provider. UMass Boston's email service uses encryption to scramble messages, making them useless if intercepted en route. Commercial email services that do not provide encryption are much less secure and should not be used to discuss or transfer confidential student information.

Avoid sending highly sensitive information via email

Because even encrypted email can be forwarded, printed or otherwise end up in an insecure location, we do not recommend sending the following information via email:

- Account names and passwords
- Sensitive personal information such as Social Security Numbers
- Files containing grades or personal data about an entire class

Do not Use Public Instant Messaging (IM)

Public instant messaging is not a secure option for communicating any sensitive information; this includes your students' grades, IDs and passwords, as well as your Social Security and bank account number.

Version Control Log

This document will be reviewed and updated annually. Please check back for current information.

Version	Date Approved	Modified By	Description of Changes
1.0	9/16/13	Linda Perrotto	