Cornell University

IT@Cornell

Course Instructors' FAQ: Managing Student Information in Cornell's IT Systems

Contents

What is the purpose of this FAQ?

This document answers course instructors' questions about protecting student information like grades and attendance sheets in Cornell's Information Technology (IT) systems (such as email or Google); these questions start halfway through the document.

Preceding the IT questions is necessary background about the types of student information course instructors may encounter covered by the Family Educational Rights and Privacy Act (FERPA) and the degree of risk associated with them.

Course instructors are partners in preventing harm due to unauthorized disclosure of student information. Thank you to the course instructors at the College of Engineering who submitted the initial questions. The answers are a collaboration between the IT Security Office Governance, Risk, and Compliance group and the Office of the University Registrar informed by the U.S. Department of Education federal government website Protecting Student Privacy and Policy 4.5, Access to Student Information.

Where can I send questions and suggestions?

For FERPA questions or requests, such as for any disclosure of information outside the institution, please contact the University Registrar.

For FAQ questions or suggestions, please submit them using this Service Desk form.

For federal government resources, see the Department of Education website Protecting Student Privacy.

Who is accountable for FERPA data use and protection at Cornell?

The University Registrar is the FERPA Data Steward, as defined in Policy 4.12, Data Stewardship and Custodianship, responsible for partnering with faculty and staff to ensure Cornell implements the Family Educational Rights and Privacy Act (FERPA) privacy protections as specified in Cornell Policy 4.5, Access to Student Information.

Anyone in the institution who generates, stores, transmits, or otherwise handles data covered by FERPA is responsible for keeping student data safe, following "reasonable methods" to prevent unauthorized disclosure.

What is FERPA?

The Family Educational Rights and Privacy Act (FERPA) is a 1974 federal law protecting the privacy of student educational records (see *What is an education record?* and *What types of information does FERPA cover?* below). FERPA safeguards student privacy by limiting who may access student records, specifying for what purpose they may access those records, and detailing what rules they must follow when accessing the data.

It also affords students the right to have access to their education records, the right to seek to have the records amended, the right to have some control over the disclosure of Personally Identifiable Information from their education records, and 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.

All educational institutions that receive federal funding, including Cornell University, must comply with FERPA. FERPA protection begins for a Cornell student on the first day of classes/semester or attendance, whichever comes first, and the student continues to be protected by FERPA for their lifetime.

The FERPA statute is found at 20 USC § 1232g (United States Code), and the FERPA regulations are found at 34 CFR Part 99 (Code of Federal Regulations).

FERPA is just one of several laws governing the regulated data Cornell must protect.

What is an education record?

An *education record* is information related to a student and maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. It includes but is not limited to:

- grades
- graded course materials (homework, exams, etc.)
- transcripts
- class lists
- audio and video with identifiable student participants
- transcripts of conversations
- student course schedules
- student financial information
- student discipline files
- personal identifiers associated with an educational record

For more detail, see *What types of information does FERPA cover?* below.

Records may be retained in any format including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and email. Source: 34 CFR § 99.2

Is it acceptable to share education records?

Yes, but education records, such as grades and other sensitive materials, must only be shared with institution officials who need them to execute their job responsibilities 34 CFR § 99.31(a)(1).

Institution (school) officials are defined in the Annual Privacy Notification Under FERPA in the University's catalog.

School officials must use "reasonable methods" to ensure they only have access to educational records in which they have legitimate educational interests. (See, *Can TAs email me grade or attendance spreadsheets?* below for what to do.)

A student may not use the right to opt out of directory information disclosures (see *What is Directory Information?* below) to prevent school officials from identifying the student by name or disclosing the student's electronic identifier (NetID) or institutional email address or email (in the format NetID@cornell.edu) in class.

Do not share educational records with any person or entity outside the institution. If such a request is made or the need to share arises, consult with the Office of the University Registrar and ensure an appropriate contract is in place to protect the data.

What types of information does FERPA cover?

The following table is a guide to the categories of information FERPA covers. Remember that this is about preventing harm to a student if the information is disclosed outside of legitimate use or stolen by someone with malicious intent. The risk depends on the specific student's situation, the information involved, who obtains access to the information, and what they intend to do with it.

If you have questions about a specific situation, contact the Office of the University Registrar.

Information Category	**Risk of Harm from Unauthorized Disclosure**
1. **Education Records** are information directly related to a student and maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. These include, but are not limited to, grades, graded materials, class lists, etc. (see *What is an education record?* above). **IMPORTANT:** The risk depends on the type of information and ranges from Moderate to High.	Contextual: It depends on the sensitivity of the record. Moderate Risk at minimum.
2. **Student Financial Information,** not limited to Financial Aid applications and records, the student's Bursar account, work-study record, cost of attendance, and satisfactory academic progress. (The Gramm-Leach-Bliley Act or GLBA also covers financial information).	High Risk
3. **High-Risk Personally Identifiable Information (PII):** FERPA doesn't explicitly describe this, but high-ri PII in Cornell's classification of regulated data includes SSN, Payment Cards, Driver's License, Visa or Passport, Bank Account numbers, and any	High Risk

Information Category	Risk of Harm from Unauthorized Disclosure
official government ID in conjunction with the person's legal name or other identifying information.	
4. **Combined Personally Identifiable Information**: Refers to situations when combined, otherwise low-risk information positively identifies a student with their educational record. An example might be some combination of NetID + Student's Full Name + Home Address + a Parent's Full Name + Phone Number + Date of Birth. If these were present in a Cornell Health record (also protected by HIPAA) or disciplinary context, it would be High Risk.	Contextual: It depends on the sensitivity of the record. Moderate Risk at minimum
5. **Directory Information** would not generally be considered harmful or an invasion of privacy if disclosed alone (not with an education record). Directory Information is defined for the institution by the University Registrar. Although this information is considered a moderate risk, the Registrar makes every effort to protect it. Do not release it outside the institution; refer all requests to the Office of the University Registrar.	Moderate Risk
6. **Suppressed Directory Information** is directory information for a student who has requested that their information not be shared. Students who request this may face increased risk due to unauthorized disclosure.	High Risk
7. **Sole Possession Records:** Sole possession records are records kept only by the maker (the author) for their personal use. For instance, notes about a student's behavior in class. The Department of Education lists them as "exempt." However, sharing them is restricted to the maker or their temporary substitute. Sharing beyond the maker or a substitute, even internally, would cause them to lose their exempt status.	It depends on what is in the notes. Moderate Risk
8. **Exempt Records** describes information not covered by FERPA. That does not mean this is not sensitive information and may be covered under other regulations like HIPAA or university policy.	Varies based on the type. Moderate Risk at minimum

What is Directory Information?

According to the U.S. Department of Education, *Directory Information* is information in an educational record that would generally not be considered harmful or an invasion

of privacy if disclosed. Directory Information is not just contact information as found in the online directory. The University Registrar defines what information is included on the University Registrar's FERPA page and shares it with students via the Annual Privacy Notification Under FERPA in the catalog.

Students can request that the institution suppress their Directory Information so it is not shared without explicit permission; however, this does not extend to preventing legitimate use in the classroom (see, ***Error! Reference source not found.****)*

Whether suppressed or not, the University Registrar protects all Directory Information. Do not release it outside the institution, and refer all requests to the Office of the University Registrar.

When is a photo or video of a student an education record under FERPA?

Information regarding sharing images, videos, and audio recordings involving students or their education records can be found in the U.S. Department of Education FAQ at studentprivacy.ed.gov. After review, if you have additional questions, contact the Office of the University Registrar.

How should I manage Personally Identifiable Information in Cornell IT Systems?

First, check the Regulated Data Chart to see if the tool is approved for Personally Identifiable Information (PII, see, *What types of information does FERPA cover?* .

Productivity software such as Microsoft 365 (previously Office 365), Box, Google Docs, and their associated products, while approved for FERPA, are **not approved** for high-risk personal identifiers, even though PII is covered under FERPA.

However, combined directory information that identifies a student is approved in these systems. For instance, you may have a student's name, email address (including the NetID), phone number, or other contact information, along with their class group assignments. Except for FERPA-suppressed PII, never store high-risk information in these systems (see, *What types of information does FERPA cover?* above), and store the minimum you need for class purposes. Where FERPA-suppressed PII has been included in a file, the entire file should be regarded as High-Risk, and appropriate care must be taken when storing and sharing High-Risk data.

Cybersecurity criminals accumulate data about individuals from multiple sources. The more information they have about a person, the more likely they are to identify a person and be able to act on that information. Therefore, everyone is responsible for minimizing the number of copies of High-Risk data and ensuring necessary occurrences are appropriately protected. The only approved place for long-term storage of high-risk PII is Cornell student systems of record, like PeopleSoft (see, *How should I share class grade books and attendance sheets if I can't use email?)*

Minimum security standards must be applied when storing FERPA data on Cornell or personally owned devices, including laptops, desktops, smartphones, tablets, etc. (see,

Can I store any FERPA data on my computer or smartphone? below)

Cornell Secure File Transfer (SFT) is the only approved service if High-Risk or other highly sensitive data must be available to another Cornell official outside an approved system. With SFT, a file is usually uploaded and downloaded to a personal device; these should be secured according to Cornell's minimum security standards (see, *Can I store any FERPA data on my computer or smartphone?* below). These files should be removed from the device as soon as the data is stored in an approved system of record like PeopleSoft.

Can I make directory information, such as name and NetID, available to students in a class for things like forming groups or finding study buddies?

Yes - if forming groups is necessary to fulfill course requirements, then it falls within a course instructor's professional responsibilities, and sharing the information is allowed.

While students can request that their directory information be suppressed (so it is not displayed, searchable, or shareable), a student may not use the right to opt out of directory information disclosures to prevent school officials from identifying the student by name or disclosing the student's electronic identifier or institutional email address in class. As long as a student is enrolled in a class, the requirements for classroom participation supersede any data restrictions placed by the student with the institution.

If a student emails me and asks for their grade, can I reply with actual exam or course grades?

Yes. You can respond to student grade inquiries if the request is made directly from a student's Cornell email address. The best practice is to refer the student to a system of record, such as a Learning Management System like Canvas or the student information system, PeopleSoft. However, disclosing grades via Cornell email is okay when a student seeks clarification or needs additional information. Grades should only be emailed to the student directly and never to third parties. Other than in the student-initiated communication above, never forward or reply to emails containing sensitive data without removing such data before transmission.

If a student communicates with you from a non-Cornell email address, the email and any attachments will be processed or hosted by systems not subject to Cornell's FERPA and security contract language and cybersecurity protections, thus increasing the risk.

Consider including guidance in your class introduction, discussion with TAs, and syllabus about the risks of using email, the institution's legal obligation to protect students' privacy and sensitive information like grades, the secure locations where grades will be posted, and preferred ways to discuss grades.

Can TAs email me grade or attendance spreadsheets?

No. Student grade rosters and attendance sheets should not be sent via email.

For what to do instead, see the answer to the question, *How should I share class grade books and attendance sheets if I can't use email?*

Remember, only share grades, attendance lists, and other education records with those who need them to perform their professional responsibilities.

How should I share class grade books and attendance sheets if I can't use email?

The recommended choices are 1) a Cornell Approved File Service if collaboration is essential or 2) Cornell's Secure File Transfer Service for one-off transfers.

To collaborate on class education records, we recommend setting up a Cornell-approved, cloud-based file library where TAs can post files in a folder for their section. The course instructor can then be granted access to the folder(s). You can use Box, Microsoft 365 (OneDrive, SharePoint, and Teams), or Google Suite (Google Docs, Drive, and Sites).

Can I store any FERPA data on my computer or smartphone?

As described above, FERPA covers High-Risk and Moderate Risk data. In general, except for temporary data transfer with Secure File Transfer, before moving to one of Cornell's systems of record, never store high-risk information.

1. **Yes, on a Certified Desktop device** for Moderate Risk FERPA records. These can be stored on a Cornell-owned Windows or Apple desktop or laptop with approved software and configuration to protect your computer from unauthorized access. You can check your device's status using the Cornell Certified Desktop Self-check App.

2. **Yes, on a Fully Encrypted Smartphone or Tablet:** While not encouraged, a fully encrypted, personally owned smartphone or tablet used only by you and never shared (say, with a family member) can be used for temporarily storing institutional data (e.g., reviewing attachments, etc.). If the device is protected by any authentication method (PIN, Password, Fingerprint, or Face recognition) for any device running IOS 7 (released in 2014) and later or Android 6 Marshmallow (released in 2015) and later, then it is automatically encrypted.

Caution! Your personally owned devices are not Cornell-supported; you are responsible for their secure operation to protect Cornell's data per the requirements listed under *Mobile Devices* in Cornell's Policy 5.10 Information Security. Institutional data must be transferred to Cornell-approved storage.

3. **No, for all other non-Cornell-owned computers** or devices, devices with non-official (not phone vendor supported and updated) versions of the Android OS or rooted devices. Be aware that vendors limit the years of security updates they

provide. Risk can increase significantly if your device no longer receives security updates.

Never store High-Risk Personally Identifiable Information: (See *What types of information does FERPA cover?* above) Grades and other educational records for class use can be stored but transferred to PeopleSoft and then deleted. Storing other records, such as graded electronic papers and email exchanges with students, is also acceptable. In any case, record retention rules apply. (See *What are the data retention rules for Educational Records?* below.)

I want to use an online tool or application for my course. However, I am worried that it is a violation of FERPA. What should I do?

If it is existing, supported software, it will be listed on the Regulated Data Chart, which shows which data can be stored in the software, and in most cases, you can sign in with your NetID email address (NetID@cornell.edu). Please note this only applies to the instance of the software managed by Cornell as it is legally subject to Cornell's contract provisions and security controls.

New acquisitions or renewals of software (free or purchased) must go through the Cornell IT Governance and Procurement process to ensure software agreements include Cornell's approved FERPA language, which describes the vendor's legal obligations under FERPA.

Caution about click-through agreements: Click-through software license agreements presented by a vendor during online purchases are bound to the person clicking it and not to the institution unless there's a contract that overrides it. Such agreements, even if purchased by a Cornell payment method such as a P-Card, can hold you personally liable for the agreement. The Procurement Office will guide you through the purchase process or contact the Division of Financial Affairs Shared Service Center for more information.

What are the data retention rules for Educational Records?

Educational records must not be retained beyond the retention period defined in Data Retention Policy 4.7. At the time of writing (October 1, 2023), Policy 4.7 sets

- Gradebook retention period to five years
- Graded course material (homework, exams, etc.) to one year after a course ends.

At the end of the retention period, these materials must be disposed of appropriately.

Note: Deletion may be insufficient to remove electronic records from a file or other data storage system. For instance, you may also need to remove it from Google Drive's Bin or OneDrive's Recycle Bin. Also, be aware that backups of your device or storage made before their removal from your device could be restored, violating the retention policy. Submit an IT Service Desk help ticket if you need assistance.

What are Sole Possession records?

Sole Possession records are notes on class activities or observations you keep for your use only.

Sharing is restricted despite being listed as exempt information by the Department of Education. They may only be shared with a temporary substitute for the record maker. Sharing beyond the maker or a substitute, even internally, would cause them to lose their exempt status.

The criteria that must be met for notes to be considered sole possession are a) a memory aid, b) private, created solely by and for the individual possessing them, and c) observations and professional opinions only.