FERPA, Handling Student Data, and Cybersecurity Concerns

General Information for the Georgia Tech Community

Nov. 2019

Purpose

- This presentation includes general information on the Family Educational Rights and Privacy Act.
- It is intended to give the campus community general guidelines about how to handle FERPA-protected student data.
- The Registrar's Office provides specialized training for offices on campus. Contact them at comment@registrar.gatech.edu if your unit wish to have more specific training.

Specific Topics

- FERPA
    - What is it?
    - To whom does it apply?
    - Why do we have to comply?
    - Rights of students
    - Education records
    - Directory information
    - Legitimate Educational Interest
- Handling student data safely
- Cybersecurity
- GDPR
- Questions

What is FERPA?

From the Family Policy Compliance Office (FPCO):

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) **is a Federal law that protects the privacy of student education records.** The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Source: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

To whom does it apply?

- Applies to all students who attend post-secondary institutions.
- **GA Tech defines "in attendance" as registered for classes.**
- Does not apply to:
  - Applicants who are denied admission.
  - Those applicants who were accepted but did not attend.

Why do we have to comply?

From the Family Policy Compliance Office (FPCO):

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. **The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.**

Source: http://www.ed.gov/policy/gen/reg/ferpa/rights_pg2.html#1

Definition of “receives funds”

(c) The Secretary considers funds to be made available to an educational agency or institution if funds under one or more of the programs referenced in paragraph (a) of this section-

(1) Are provided to the agency or institution by grant, cooperative agreement, contract, subgrant, or subcontract;

or (2) Are provided to students attending the agency or institution and the funds may be paid to the agency or institution by those students for educational purposes, such as under the Pell Grant Program and the Guaranteed Student Loan Program (Titles IV-A-l and IV-B, respectively, of the Higher Education Act of 1965, as amended).

Source: http://www.ed.gov/policy/gen/reg/ferpa/rights_pg2.html#1

What does it do?

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a **Federal law that protects the privacy of student education records.** Institutions are required to notify eligible students about their rights under FERPA.
  - The Family Educational Rights and Privacy Act (FERPA) **affords students certain rights with respect to their education records.**
  - They are:
    - The right to inspect and review the student's education records;
    - The right to request the amendment of the student's education records that the student believes are inaccurate or misleading;
    - 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;
    - The right to file a complaint with the U.S. Department of Education concerning alleged failures by the Georgia Institute of Technology to comply with the requirements of FERPA.

Education Records

“Education records”

- The term means those records that are:
  - (1) Directly related to a student; and
  - (2) Maintained by an educational agency or institution or by a party acting for the agency or institution.

Source: http://www.ed.gov/policy/gen/reg/ferpa/rights_pg4.html#3

Different Formats

- Education records are stored in different formats.
  - Olden days – paper
  - Electronic age –
    - Databases
    - Back-ups of databases
    - Images of documents
    - PDF files
    - Banner
    - Other systems used in addition to Banner

Documents in our imaging system are “education records”.

International Students

- International students have the same rights as domestic students under FERPA.
  - inspect their records
  - request amendments
  - protect privacy
- International students consent to release of their information to certain governmental agencies on various forms.
  - Department of Homeland Security

Releasing Information

- Permitting access to or the release of personally identifiable information to any party. This includes any communication by oral, written, electronic or any other means.
- Schools are not allowed to disclose information (other than “**Directory Information**”) without the student’s written consent except under very limited conditions.

Directory Information

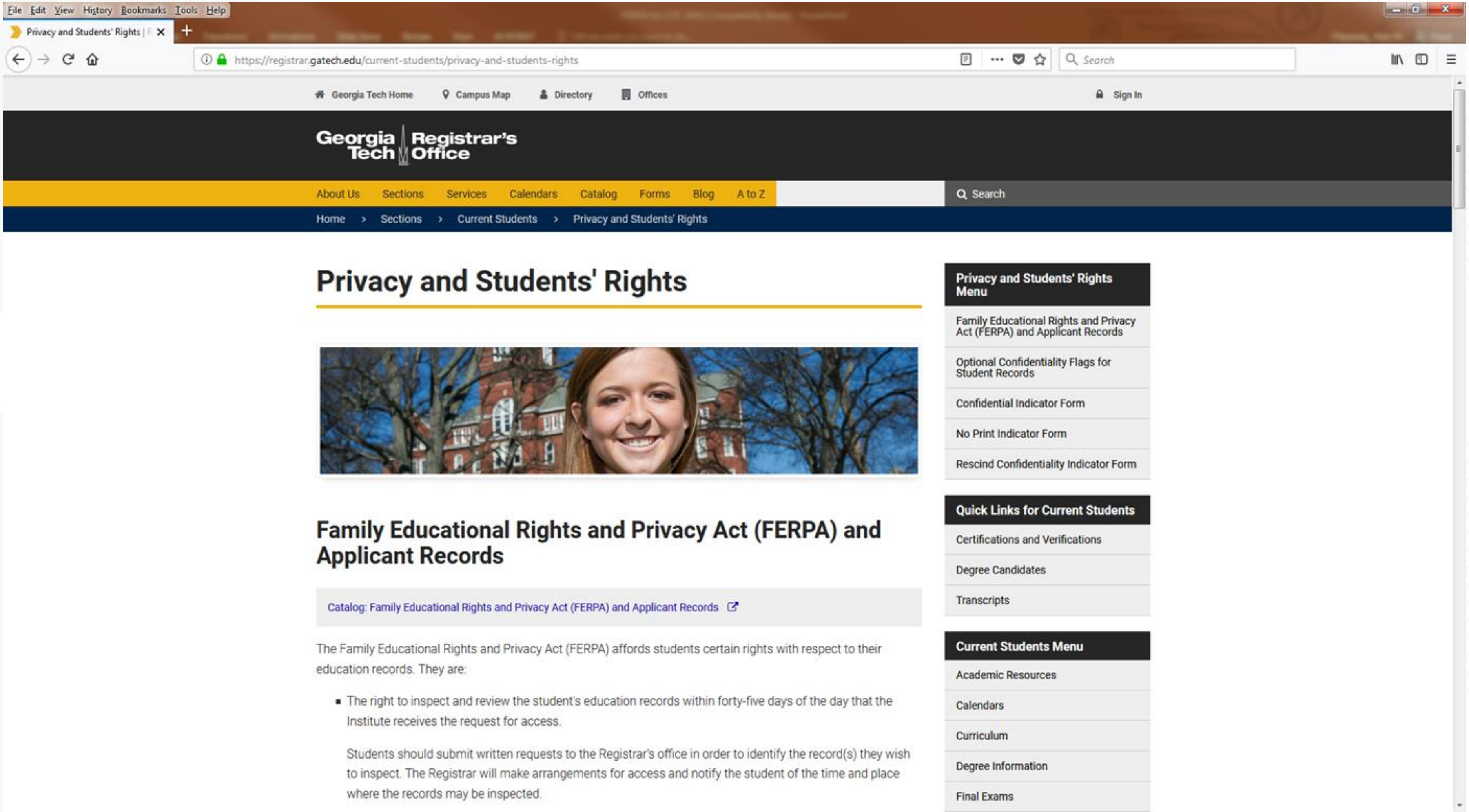
Annual Notice of Directory Information Consents

“Directory Information” is information not generally considered harmful or an invasion of privacy if disclosed. Effective November 12, 2016, the Georgia Institute of Technology considers the following information to be directory information:

- Name, address (including GT email address), and telephone listing
- Level (graduate or undergraduate)
- Field of study
- Enrollment status (full-time, part-time, less than part-time)
- Dates of attendance
- Degrees with associated honors and designations, and date(s) awarded
- Anticipated date of graduation
- Participation in NCAA Division I sports, including terms of team membership

There is more information on the Registrar’s website at: http://catalog.gatech.edu/policies/ferpa/

Confidentiality


File Edit View History Bookmarks Tools Help
Privacy and Students' Rights | F
https://registrar.gatech.edu/current-students/privacy-and-students-rights
Search
Georgia Tech Home
Campus Map
Directory
Offices
Sign In
Georgia Tech Registrar's Office
About Us
Sections
Services
Calendars
Catalog
Forms
Blog
A to Z
Search
Home › Sections › Current Students › Privacy and Students' Rights

Privacy and Students' Rights

Family Educational Rights and Privacy Act (FERPA) and Applicant Records

Catalog: Family Educational Rights and Privacy Act (FERPA) and Applicant Records

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

- The right to inspect and review the student's education records within forty-five days of the day that the Institute receives the request for access.

  Students should submit written requests to the Registrar's office in order to identify the record(s) they wish to inspect. The Registrar will make arrangements for access and notify the student of the time and place where the records may be inspected.

Privacy and Students' Rights Menu

- Family Educational Rights and Privacy Act (FERPA) and Applicant Records
- Optional Confidentiality Flags for Student Records
- Confidential Indicator Form
- No Print Indicator Form
- Rescind Confidentiality Indicator Form

Quick Links for Current Students

- Certifications and Verifications
- Degree Candidates
- Transcripts

Current Students Menu

- Academic Resources
- Calendars
- Curriculum
- Degree Information
- Final Exams

Confidentiality

- Students have the right to request that their names not appear in the online campus directory.
- Students also have the right to request confidentiality.
- Requests are handled in the Registrar’s Office and the student information system is flagged upon receipt of the signed and dated form.
- A revised form is required if the student wishes to revoke the request.
- Any questions should be directed to comments@registrar.gatech.edu.

Legitimate Educational Interest

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.** A school official is a person whether volunteering for or **employed by the Institute in an administrative, supervisory, academic or research, or support staff position** (including law enforcement unit personnel and health staff); a person or company with whom the Institute has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

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 responsibility.

Legitimate Educational Interest

This means that you have access to FERPA-protected student data because your job requires you to have it in order to preform your duties as an employee of Georgia Tech.

- Because the requirements of individual jobs vary, so does the "role" of the employee in regard to what they can access or handle in regard to student data.
    - Remain mindful of this and do not request access to data elements that you do not need to perform your job.
    - Remain mindful of this as well while interacting with your colleagues. The fact that you may have access to certain data elements does not mean that all your colleagues share your "role." In working with your colleagues, it is sometimes necessary to share student information. Do so carefully and thoughtfully bearing in mind the question and the assistance that you are trying to provide for the student.
    - Remain aware that if you take another position on campus or even within your unit, your "role" may change, meaning that your level of access may also change.
    - Remain mindful that accessing student information because you may be curious about it is not a legitimate reason. Any access or handling of FERPA-protected student data must be related to your job duties.

Type of Access

- There are **three types of users** of student data that we need to address:
- Those who have general access to FERPA-protected student data to do their jobs
- Those who have general access to FERPA-protected student data to do their jobs and who run reports and/or provide data to other staff members
- Those who may not have general access to FERPA-protected student data, but who handle it in some way in the process of doing their jobs
    - This can be described more succinctly as:
        - General access staff
        - General access staff who also write/run reports
        - No general access staff who still handle student data

Type of Access

- General access
  - Has access to Banner
  - Has access to GT reports
  - Has access to student data through other products or means (examples might be Grades First, Handshake)
- General access staff who also write/run reports
  - Has access to Banner
  - Has access to GT reports
  - Has access to student data through other products or means
  - Has a job responsibility to write or run reports or provides student data to others
- No General Access
  - Has no access to Banner
  - Has no access to GT reports
  - Has no access to student data through other products or means
  - ***Does*** handle student data as provided by another staff member.

General Access – Best Practices

If you are someone who accessed student data or handles it in any way:

- Use it only for the purpose of performing your duties.
- Do not share it with a third-party, internal or external.
- Do not share it with other staff members unless you are working together on a project or task that requires you to discuss or handle the data.
- Do not leave reports out in open areas where others could see it, especially if you work in an area where there is student traffic.
- Do not load student data onto a laptop or a thumb drive and cart it around with you.
- Do not email student data to anyone without taking some precautions.
- Do not use email at all if you have other options.
- When requesting a report or list, always ask for exactly what you need for that particular task or project and nothing more.
  - Always check the report or list before you do anything with it to ensure that there is no extraneous data included.

General access and write/run reports…

If you are someone who runs reports or extracts data for others:

- When someone asks you to run a report, they need to tell you exactly which data elements they need.
  - They need to tell you how they are going to use the information.
  - If the data elements they are requesting seem inconsistent with how they are going to use the information, question it.
  - Give them only what they requested, and no more.
- Review your spreadsheet or printout before you pass it on to the requestor to make certain that you have not inadvertently given them more than they need, or something that you intended for someone else.
- If you use email, and this is not the best option, you should password protect the spreadsheet. You send the password in a separate email (we will get more into this in a few moments).

General access and write/run reports…

If you are someone who runs reports or extracts data for others, continued…

- Remain aware that there are offices on campus can prepare custom reports as needed. It is better to ask for a custom report if getting the information yourself is cumbersome or rather than using GT reports and gathering more information than you actually need.
  - Contact the Registrar's Office at comments@registrar.gatech.edu for more information.
- As you are working with your unit on new technologies that are focused on communication with students, or on providing internal communication within your office, bear all of the above in mind.
- **The data custodians on campus expect you to safeguard student data or any other kind of protected data in the same way that you would protect your own personal data.**

No general access…

- If you handle FERPA-protected student data in any way to perform your job, it is your responsibility to handle it safely.
- It doesn’t matter whether you have Banner or GT Reports access or any other kind of access to systems used on campus outside of Banner; if you handle student data, you have to be mindful of doing so in a safe manner.
- Even if the only student data to which you have access is that which someone else has provided for you, you have to follow good business practices in how you use it to perform your job duties.
- Your responsibility is the same as that of your colleagues and you will be held accountable for handling student data appropriately.
- If you have any questions at any time in regard to your responsibilities under FERPA, see your supervisor immediately.

Accessing Student Records in Banner

- Access to student records in Banner is based on the requirements of your job.
  - When access is granted, a role is created that dictates which forms you can view and this is based on your need to know.
  - There is no data element level access in Banner, so you may see information on some of the forms that is not needed for you to conduct your duties.
  - We operate on the honor system in that regard.
  - Keep this in mind and stay focused on what you need to access to perform your duties.
  - Do not log into Banner and leave your desk. Banner will time out, but if you leave your desk for any period of time, log out.
  - If someone who does not have Banner access asks you to look for something, make sure you understand whether it is a legitimate request before acting.

Emailing reports versus using One-Drive or DropBox

- If you prepare a report for someone, you will have to decide how to send it to them.
- Many offices on campus use email to transmit reports.
- Instead, use One-Drive or DropBox to share information. This secures it and keeps it out of the email environment.
- We are recommending that your group become familiar with One-Drive and DropBox and move away from email.
- If you must use email for any reason, keep the following in mind:
- Double check the email address of the requestor to make sure the report is going to the right person.
- Double check the attachment and make sure it is the right one.
- Double check the attachment to make sure that it contains only the information that are requested.
- Password protect the attachment.

Sending mass emails to students…

- Use existing listservs that have already been vetting to reach the right population.
- Make sure you suppress the recipient list.
- If you need a special report to identify a specific population, avoid output that offers more data elements than are actually needed.
- Make sure that you don’t accidentally add an attachment.
- **Do no use the forward function.** Using “forward” to send the email may only add an opportunity for something to be sent accidentally.

Lading FERPA-protected information onto laptops, thumb drives, or other portable devices:

DON’T DO IT!

Cybersecurity Standards at Tech

- You are expected to be aware of and to abide by Georgia Tech policies:
  - Cyber Security Policy
  - Data Privacy Policy
  - Password Policy
- Information can be found on the OIT website at:
  - https://oit.gatech.edu

Cybersecurity Standards for Tech Employees

Employees

- Employees and student employees are responsible for securing all data and IT equipment to which they have access. This extends to personally owned devices that access Georgia Tech resources. Employees are to secure their accounts and passwords to be compliant with the Password Policy.

Responsibilities:

- All employees are to secure their machines when they walk away – which means to lock their workstations, laptops or any other IT resources.
- Laptops and other portable IT hardware are to be stored physically secured in public areas where it is not easily accessible to public.
- Passwords are to be treated as only the sole knowledge of the employee and no one else. Passwords are also not to be readily available physically nor visibly.
- In the event of stolen Institute IT resources, notify the authorities, management, and system administrator.

Cybersecurity Standards for the Campus

System Administrator

- The system administrator professionally manages all Institute owned IT resources and by the unit technical support team unless prevailing regulations dictate otherwise. The system administrator is responsible for maintenance of the machine and must be accessible to the unit technical support team for incidents unless legal restrictions prohibit access.
- Negligent management of Institute owned IT resources such as unauthorized user access or a data breach may result in the loss of system administration privileges.

Responsibilities:

- Complying with all relevant Institute IT policies and procedures.
- Performing cyber security self-assessment for administered Enrollment Services IT resources
- Enrollment Services' established security standards that are managed by the systems administrator as follows:
  - All systems are to have FireEye HX agent.
  - All systems are to be managed through a central Endpoint management agent.
    - Active Directory (Microsoft Windows)

      JAMF (Apple iOS and Mac OS)

Cybersecurity Standards for the Campus

Responsibilities (System Administrator, continued):

- System administrators are to have a separate CSR admin account
- Backup solutions
- All systems are to have whole disk encryptions
  - BitLocker (Microsoft Windows)
  - FileVault (Apple Mac OS)

Enforcement:

- Violations of these standards may result in loss of Georgia Tech system and network user privileges, and/or disciplinary action, up to and including termination or expulsion as outlined in applicable Georgia Tech policies. Progressive discipline could also be a consequence of violating these standards.
  - 1st Violation: A warning, as long as it does not occur in a public area.
  - 2nd Violation: Lock time is lowered and loss of access to multi-user computers for a set period.
  - 3rd Violation: Lock time is dramatically lowered, loss of access to multi-user computers and departmental resources such as file server access will be disconnected.

Cybersecurity Standards for the Campus

What does this mean for me?

- Your desktop support or computer services representative requires you to do certain things a certain way for a reason.
  - There are campus policies that dictate how your access is managed and how you are expected to handle that access appropriately and safely.
  - Follow the instructions of your IT professionals at all times.
  - If you have any questions, go to your desktop support folks or your IT representatives. It is better to ask than to be sorry.
- Bear in mind that some of the safeguards that are in place may take up your time occasionally, such as locking your workstation when you leave your work area. Yes, you will have to log back in, but failure to lock it means that anyone visiting your workstation could decide to “be you” even for a short time and behave inappropriately.
  - If something happens under your log-in, you are responsible.
- This focus is on student data protected by FERPA, but some of us also handle other kinds of protected data.
  - Remain aware of the kinds of data that you handle in the process of doing your job.
  - Don’t make any assumptions about what is appropriate or not.
  - Ask questions.

Telephone Calls

- Some of our interaction with students comes with over the telephone.
  - Remain mindful that it is difficult to ascertain identity by telephone.
  - Ask a sufficient number of questions that you can verify to be comfortable that the caller is legitimate.
  - If you feel uncomfortable, ask that the student visit in person.
  - If the caller is a distance education student, ask a sufficient number of questions to be comfortable in talking with the caller.
  - You can often provide assistance and useful information without saying anything specific about a student’s education record. Some of the calls we receive are about academic policies or procedures that can be discussed with anyone, without revealing any specific, personally identifiable information.
  - If the situation warrants it, we can require written, signed, and dated requests for information.
  - Even though “directory information” is considered public, and not harmful if given out, we have the option to provide it, but we do not have to do so.

Visitors in the Office

- Do not send students or other visitors back into the office without escort.
- Always lock your desktop when you step out, for whatever reason.
- If you bring a student or other visitor back to your office, make sure you are not exposing anything either on your desk or on your monitor.
- If you are working with students or other visitors in another location, such as at FASET or a help session elsewhere in the building, remain aware of what you are carrying with you that might contain sensitive information.

Proper Use of Survey Instruments

- Qualtrics is the only officially licensed survey tool at Tech.
- It is not recommended that you use other tools such as SurveyMonkey where FERPA protected or other protected information is involved.
- Even when utilizing Qualtrics, you should be thoughtful about what identification you are asking the responder to provide.
  - If they are logging in with their CAS credentials, there would be no need to ask them for name, GT ID, email address etc.
  - If, for the purposes of your research, you need personally identifiable information, limit it to exactly what you need and no more.
  - Always limit the questions or information requested to exactly what you need and no more.
  - Your manager will follow up with more discussions on the use of survey instruments.

Georgia Tech
CREATING THE NEXT

Instructional Faculty

- Some important reminders for instructional faculty:
  - Students have a right to review their own information, including grades, but they do not have a right to view the information, including grades, of other students
    - Do not put graded homeworks, exams, papers, etc. in a box outside your office. Leave them in a secured place with someone to check GT IDs before handing them back to students.
    - Do not put graded homeworks, exams, papers, etc. on a desk in your classroom so that students have to look through them to find their own material. Find a few moments before or after class to hand them back to the students.
    - Do not post lists of grades or other information in a public area.
    - Remain mindful of confidentiality when having conversations with individual students.
    - Do not pass graded homeworks, exams, or papers, etc. back to students in class in a manner in which they can see each other's grades.
    - If you teach online courses, there is additional information on the Registrar's website at: https://registrar.gatech.edu/ferpa/privacy-checklist-for-online-courses
    - If you are using Canvas and have questions, contact the Canvas team at: https://canvas.gatech.edu/.

Parent Access

- Parents of elementary and secondary students have more access to information than they do for their college student. Remain mindful of the following:
  - Once a student enrolls in classes at Tech, their records are protected by FERPA and their parents or guardians no longer have access.
  - In rare cases of student illness and/or personal accidents, parents should be referred to the Dean of Students' office to discuss their student's records.
  - Some institutions allow students to sign a blanket FERPA waiver so that students can have view access to student records. Georgia Tech does not. It is our choice under the law to allow this or not. We have chosen to not do so.
    - Parents often think that if they claim the student on their income tax, they have automatic access to student record information. This is not the case.
    - Georgia Tech **does not** issue blanket waivers of FERPA for any reason.
    - Refer any related questions to comments@registrar.gatech.edu.

EU GDPR – what is that?

European Union General Data Protection Regulation Privacy Notice

- This is the Georgia Institute of Technology's (Georgia Tech) Office of the Registrar privacy and legal notice for compliance with the European Union General Data Protection Regulation ("EU GDPR"). For more information regarding the EU GDPR, please review Georgia Tech's EU General Data Protection Regulation Compliance Policy.

https://registrar.gatech.edu/eu-gdpr/policy

Why do we care?

- It’s our job.
- It’s the law.
- Data spills and breaches can have negative impacts on our students.
- Data spills and breaches damage our reputation and credibility.
- Data breaches and exposures take up a lot of time and resources, are therefore costly, and take our attention away from value-added projects.

Consequences

- Staff who do not abide by these rules may be subject to progressive disciplinary action.
- Failure to comply with FERPA-related responsibilities could result in disciplinary action up to and including termination of employment.

Resources

- Related web sites
  - https://registrar.gatech.edu/ferpa
  - https://www2.ed.gov/policy/gen/guid/fpco/index.html
  - https://registrar.gatech.edu/eu-gdpr
  - https://www.usg.edu/records_management/schedules/usgprint/934
  - https://www.usg.edu/siteinfo/web_privacy_policy