FERPA: Securely storing student data

The Family Educational Rights and Privacy Act (FERPA) is legislation enacted to protect the privacy of students. It is important to understand the types of data that are protected under FERPA and how to store that data securely.

The diagram below highlights some types of data that must be protected under FERPA, including a decision guide to help instructors understand which applications and devices can be used in different situations. For example, Slack and Discord would be appropriate to use for collaborative student assignments, but it would not be an appropriate place for instructors to share student grades.

Please note that this diagram is not comprehensive. If you are unsure about whether something constitutes FERPA-protected data or where it can be stored, please contact the Campus Help Desk (801-581-4000, option 1) or the Information Security Office's Governance, Risk & Compliance (ISO-GRC) team at iso-grc@utah.edu. To learn more about FERPA, please visit the FERPA Primer: The Basics and Beyond website.

Does it contain FERPA-protected data?

Any student record data that is personally identifiable and related to a student — including communications between a student and a university official — is considered FERPA-protected and should not be transmitted or stored on the apps or devices listed in the No category below. FERPA-protected student record data includes but is not limited to:

- Student name*
- Student uNID*
- Grades
- GPA
- Transcripts
- Academic evaluations
- Attendance
- Disciplinary action
- Resumes and letters of reference*

*Only constitutes FERPA when combined with one or more of the other FERPA-protected data types.

Yes

Protected FERPA data may only be stored in the following locations:

- Adobe Creative Cloud*
- Canvas*
- G Suite*
- Microsoft Office 365, including Teams*
- uBox*
- UMail*
- Zoom*
- Personally-owned and encrypted devices that comply with University Policy 4-004
- University-issued and encrypted devices, such as laptops, tablets, smartphones, and flash drives

*Only use official University of Utah-issued accounts that require you to login with your uNID, password, and Duo app or token. Be sure only authorized people can view the data.

No

If no protected FERPA data is involved, then it is acceptable to use just about any app or device, including:

- iCloud
- Personal email accounts
- Personal file storage accounts, such as Dropbox
- Slack and similar collaboration tools
- Personally-owned devices, such as laptops, smartphones, and flash drives

Resources

- Office of the Registrar's Faculty & Staff FERPA Resources page
- Policy 4-004: University of Utah Information Security Policy
- U.S. Department of Education's FERPA website: Protecting Student Privacy

INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH
it.utah.edu | security.it.utah.edu