

UF IT Standards for Data Use

Limitations of UF Private Educational Records



Authority

This standard was enacted by the UF Senior Vice President for Administration and the UF Interim Chief Information Officer on July 10, 2008 [6]. It was approved by the UF Vice President of Student Affairs, UF Chief Privacy Officer and UF General Counsel.

What Constitutes the Private Educational Record?

Data protected by the Family Educational Rights and Privacy Act (FERPA) [1], the Florida student records statutes [3,4] and the UF rule for confidentiality of student records [5] is called the UF Private Educational Record (UF-PER) by the University of Florida. UF-PER is information that can be used to easily trace a student's identity.

Any and all parts of the student record are UF-PER for students who request and receive an authorized "privacy hold" through the UF Registrar's office. For all other students, most information in the student record is UF-PER except the following:

- Student name
- Local/permanent addresses/email address
- Telephone number(s)
- Class and college
- Major
- Enrollment status (e.g., undergraduate or graduate level; full time or part time)
- Dates of attendance at UF
- Degrees and awards received at UF
- Most recent previous educational institution attended
- Weight and height of university athletes

Limitations of UF-PER Use

1. Storage on and transmission between servers and desktops managed by UF IT Workers is permitted only for authorized roles. Encryption is recommended.
2. Storage on backup media is permitted only for authorized roles. Easily portable backup media should be encrypted. Student records are exempt from Florida records retention law [4].
3. Storage on personally managed computers, portable computers, and removable media should be avoided and needs approval by the Data Principal (Dean, Director or Department Chair), even for authorized roles. Where such usage is unavoidable, strong encryption is required.
4. Transmission involving non-UF servers and networks should be avoided and needs approval by the DDD, even for authorized roles. Encryption is required.
5. Anyone with access to UF-PER must attend UF-sanctioned data protection training and must agree to comply with UF data protection requirements.
6. Removal of UF-PER from UF premises requires Data Principal approval [2].
7. Any alternatives or exceptions to these limitations must be approved by the Data Principal. They should be rare and they must be documented.

Bibliography

[1] Family Educational Rights and Privacy Act:

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

[2] UF Privacy Policy: <http://privacy.ufl.edu/>

[3] Florida Statute 1002.22, Student and Parental Rights and Educational Choices:

http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch1002/SEC22.HTM&Title=-%3E2007-%3ECh1002-%3ESection%2022#1002.22

[4] Florida Statute 1006.52, Student Records:

http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch1006/SEC52.HTM&Title=-%3E2007-%3ECh1006-%3ESection%2052#1006.52

[5] UF Rule 6C1-4.007 Student Affairs: Confidentiality of Student Records:

<http://regulations.ufl.edu/chapter4/4007.pdf>

[6] DDD announcement of this standard,

<http://lists.ufl.edu/cgi-bin/wa?A2=ind08&L=DDD-L&P=R35323&I=-3>