Privacy

I. Abstract

The University is subject to numerous federal and state laws that protect the privacy of certain types of information. While the laws on the books still often refer to the privacy and confidentiality of "records," more often than not, the more recently promulgated state and federal laws recognize that privacy and confidentiality must attach to certain types of "information," regardless of the form this information takes, or how it is maintained. Obviously, the subject of privacy is too broad to tackle in a single module. This module therefore focuses on some considerations to keep in mind as we receive, create, or maintain sensitive/critical information. Two separate modules then provide additional information on information technology security and the privacy and confidentiality of student education records.

II. Helpful Contact Information

University Compliance Office*	IT Security Office	Office of the General Counsel	Academic Affairs
PC 520	PC 534A	PC 520	PC 526
Ext. 7-2216	Ext. 7-1366	Ext. 7-2106	Ext. 7-2151

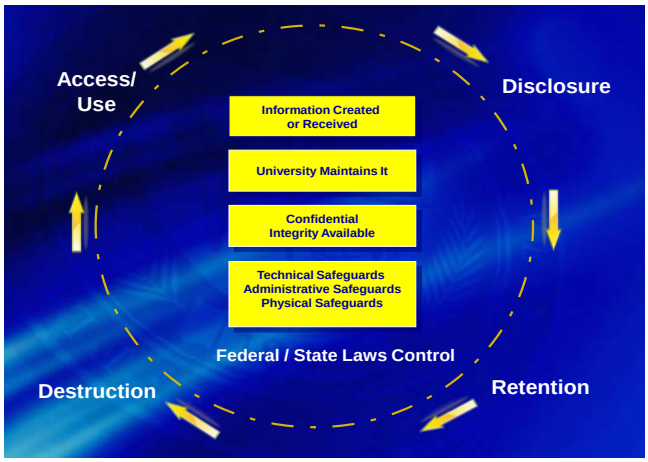
*The University Compliance Officer is the University's Interim Privacy Officer.

III. Rules of the Road

a. Federal and Florida laws protect the privacy and confidentiality of certain information that the University creates, receives and maintains.
b. Examples of protected sensitive/confidential information include, without limitation:
    i. Social security numbers
    ii. Student education records
    iii. Personally identifiable financial information
    iv. Trade secrets
    v. Health information
        1. Genetics
        2. HIV/AIDS
        3. substance abuse
        4. mental health
        5. physical health
    vi. National security information
    vii. Employment records
        1. criminal background checks
        2. health information
        3. occupational exposure records

Privacy

c. To the extent that the information that is being received, created or maintained is protected by law, this protection would have to extend to the entire cycle covering access/use, disclosure, retention and ultimate destruction:



d. Thus, to ensure the privacy of sensitive/confidential information, the University has in place administrative, technical and physical safeguards. Examples of each follow:

i. Administrative Safeguards:
   1. Policies/procedures in place
   2. Education/training to learn legal parameters and continue to reinforce scope of our responsibilities

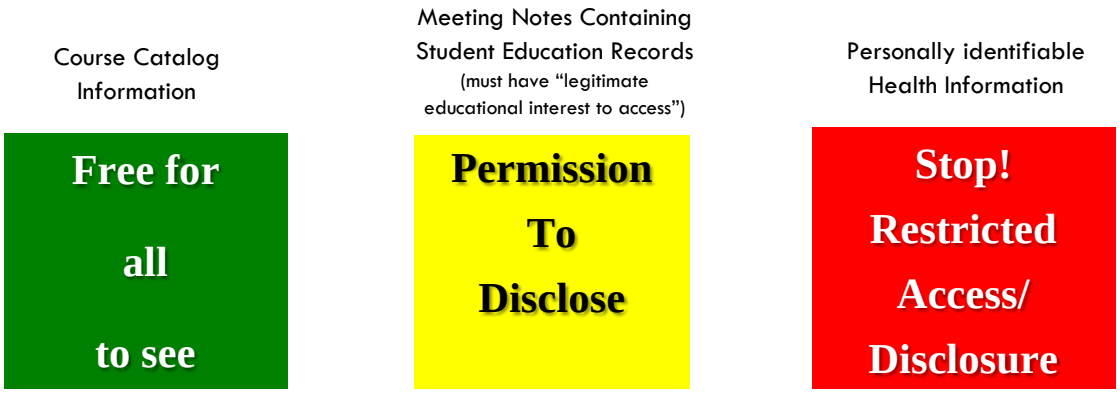
ii. Physical Safeguards:
   1. Store "records" in office space where
      a. access can be monitored or restricted
      b. records can be locked
      c. records are not in plain view
      d. secure computing facility

iii. Technical Safeguards:
   1. Screen Savers
   2. Firewalls
   3. Strong passwords
   4. System management
   5. Virtual boundaries

e. In general, then, when dealing with information created, received or maintained by the institution, faculty and staff should determine what type of information is at stake: Is it in the nature of course or catalog information free for all to see? Is it in the nature of notes or documentation provided at meeting containing student education record information

such as grade point averages? Is it highly sensitive information that cannot/should not be taken out of the office/location/computer where originally stored or accessed without appropriate safeguards such as health, mental health, or substance abuse information?

Examples:



f. Some helpful hints in dealing with information created, received or maintained by the institution include, without limitation:

- Know what type of information you are dealing with
- As an employee, access only if necessary to perform a job function and you have been duly authorized
- Review policies/procedures on how to access, use and disclose this information
- Remember that Access ≠ Disclosure: Make sure you have appropriate authority to disclose
- Each incident of data use should be evaluated individually
- Attend training/educational opportunities
- Do not hesitate to raise questions or concerns