

## Handling Restricted Student Data

Examples of Restricted Student Data are:

- SSN - May not be released, emailed or sent via campus mail, postal service, Fed Ex, etc. Refer to matrix below. *(Note: You may not use the student's full or partial student identification number in correspondence, reports or transmission).*
- Student Restricted Directory Information
  - RESTR-HOME, home address and telephone listing may not be released
  - RESTR-LOCL, local address and telephone listing may not be released
  - RESTR-ADDR, all address and phone listings may not be released
  - RESTR-PHON, all phone listings may not be released
  - RESTR-SCHOOL, school, field of study, credit hours, or classification may not be released
  - RESTR-DEGS, degrees and honors received may not be released
  - RESTRICTED, no information at all may be released
- Financial Aid information
- Immunization records
- Credit card information, application fees, check information
- Patient test results information
- Test scores either internal or from standardized tests such as SAT, ACT
- Plan of study
- Fellowship awards
- Minority student information
- Student exam schedule
- Student's class schedule information
- Grades may not be released. May not be posted when associated with personally identifiable information such as SSN.
- GPA or grade information may not be released. May be released to an employer or potential employer only if the student has signed a statement allowing the release of resume information to an employer or potential employer AND the student's resume contains the specific index or grade information requested. Additional information about any education records or personally identifiable information may not be supplied without the written consent of the student. Verification of specific information supplied by the student on the resume may be permissible. *Please be aware that using even a portion of the student identification number when posting grades can raise confidentiality concerns. Randomly assigned, unique identification numbers are the expected method. A strongly recommended format for the provision of grades is the use of a system where students can access only their scores via a password.*
- Encumbrance information
- Transcripts
- Student Resume information
- Medical records
- Psychological reports
- Clinical dictation for transcribing into voice data format

## D-R-A-F-T As of: September 16, 2005

### Handling Printed Restricted Data

1. Labeling	Documents should be labeled as "Confidential."
2. Duplication	Receiver of document containing restricted information must not further distribute without permission.
3. Mailing (internal)	Acceptable if mailbox is maintained within the same office. Information should be in an envelope marked "confidential". Preferred method of delivery is by hand even within the same office.
4. Mailing (external)	Do <u>not</u> mail outside the area. Preferred method of delivery is to hand deliver paper, disk, CD. (Note: <i>Partial student identification number does not reduce risk.</i> ) <i>Fed Express etc., is not considered a safe method of delivery unless the data is encrypted on the CD or disk being sent.</i>
5. Destruction	Destroy beyond recognition (i.e. shredding).

### Handling Electronically Stored Data

1. Storage on removable media (i.e. CD's, diskettes)	Not preferred. However, in cases where information must be archived, or transmitted outside the university, encrypting the information on the disk or CD is required.
2. Printing of data	Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing.
3. Storage on fixed media (i.e., server) with access controls (password protected)	Encryption not required
4. Storage on fixed media (i.e., hard drive) without access controls, but not accessible via the web	Not recommended, very high risk. Preferred method of storage is in item 3 above.

### Handling Restricted Transmitted Data

1. Fax	Machine must have limited access. It is recommended that the receiver is present when the Fax is being transmitted.
2. By Voice Mail	Do not leave restricted information in voice mail message. Request call back.
3. By Wireless or cellular technology	Do not transmit.
4. Other electronic transmissions (email, ftp etc)	Encryption required.

For the complete data handling matrix go to  
<http://www.itap.purdue.edu/security/policies/procedures/dataHandling.cfm>

**D-R-A-F-T** As of: September 16, 2005

*NOTE: the on-line matrix is not fully up to date to comply with recent policy and procedure changes and is currently under review.*