PURDUE
UNIVERSITY

COLLEGE OF EDUCATION
Education IT

Dear Colleagues in the College of Education:

On July 1, 2006 several new Indiana laws related to how Sensitive and Restricted data is to be handled come into effect. This has also led to some changes and clarifications of Purdue University policies regarding these issues. The following is a brief summary of the policies and procedures moving forward.

Of immediate note are five important considerations:
(see below for definitions of Restricted and Sensitive data)

1. **Restricted data that is unencrypted may not be stored on file servers, workstations, or portable electronic devices. All Restricted data stored on these devices must be encrypted.**

2. **Sensitive data is required to be encrypted when stored on portable devices or removable media (e.g. CDROM, Flash Drives, Portable Hard Disks).**

3. **Sensitive and Restricted data may not be stored on personal computer equipment at home.**

4. **If you own Social Security Numbers you must submit an SSN Policy Exception form to the ITaP Security and Privacy group.**

5. **If you own any Restricted data please contact the Education IT team for assistance in handling that data.**

Please avoid backing up Purdue Student Data along with your own personal data backup. If you feel you have a need to back up Purdue Student Data, please contact the Education IT team for an advanced backup solution that includes encryption.

What is Restricted Student Data?
Restricted -- Information protected because of protective statutes, policies or regulations. This level also represents information that isn't by default protected by legal statue, but for which the Information Owner has exercised their right to restrict access.

Specific Examples of Restricted Student Data are:

- **SSN** - May not be released, emailed or sent via campus mail, postal service, Fed Ex, etc. *(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

Beering Hall of Liberal Arts and Education • 100 N. University St. • West Lafayette, IN 47907-2098
(765) 494-2658 • Fax (765) 494-5832 • edit@purdue.edu • www.education.purdue.edu/edit

  - RESTR-DEGS, degrees and honors received may not be released
  - RESTRICTED, no information at all may be released
- **Class schedule information**
- Clinical dictation for transcribing into voice data format
- **Confidential letters of recommendation**
- Credit Bureau information
- Credit card information, application fees, check information
- Criminal investigation information
- Deceased students
- Disability information
- Discipline information
- Donor information
- Encumbrance information
- Exam schedule
- **Fellowship awards**
- Financial Aid information
- Financial information of students and or parents
- Fraudulent records information
- **Grades may not be released. Also, they may not be posted when associated with personally identifiable information such as SSN or PUID.**
- **GPA or grade information** may not be released. *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.*
- Insurance information
- Litigation information via internal staff and 3rd party service providers
- Medical records
- Minority student information
- Patient test results information
- **Plan of study**
- Psychological reports
- Resume information
- Salary information collected from former students
- Subpoenas for student records
- Test scores either internal or from standardized tests such as SAT, ACT
- Transcripts
- Veterans' records
- Witness protection program participants

What is Sensitive Student Data?
Sensitive -- Information whose access must be guarded due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a civil statute requiring this protection.

Specific Examples of Sensitive Student Data Include:

- **PUID:** PUID is a number that should have no value to anyone outside Purdue University. It isn't considered to be at the same level of security as SSN, but it IS considered to be Sensitive information. The PUID alone cannot be used to gain access to confidential information, such as grades. However, when used with the appropriate authentication credentials, it can provide access to grades as well as other confidential information.
- **Paper Admissions Applications**: Applicant information is entered into the Student Information system. This information is used to make an admissions decision and is the first step in creating a student's educational/academic record should s/he enroll at Purdue. While admissions data is not covered under FERPA, it is considered Sensitive information and is treated as such. The information is stored in non-public areas and access to it is guarded.
- **Electronic Admissions Applications**: Students view and interact with static and dynamic web pages stored on a secured web server. Students are allowed to save their electronic application and are given access to that application via access controls. Once an electronic application is submitted student access to the application is not available. Web applications are extracted and loaded to the Student Information system and a printed copy of the application is generated.
- **Prospective Student Contact**: Information collected on contact cards or received from outside vendors is entered into the Student Contact System (SCS). This information is used, in an electronic format, for such things as sending information about Purdue schools, financial aid information and invitations to recruitment events to prospective students. Once the data is entered from the contact cards, the cards are recycled and destroyed.

How should student Data be handled?
Sensitive and Restricted data should be handled with the utmost care. The following table describes example of how electronic (computer based) student data should be stored. Pay special attention to the fact that **Sensitive data needs to be encrypted when stored on removable media** such as CDROM, DVD, Flash Drives, or External Hard Drives and **Restricted data needs to always be encrypted**. If you have questions about this, contact The Education IT team at edit@purdue.edu. Full details on this policy can be found at: http://www.purdue.edu/SSTA/datasteward/security/files/Elec%20Stored.pdf

Action	Public	Sensitive	Restricted
Storage on fixed media (i.e. server, network drive) with access controls (password protected)	No special requirements	Encryption not required, but recommended.	Encryption of SSN information required and access limited to those who have a business requirement for the information
Storage on removable media (i.e. CD's, diskettes, zip drives, external hard drives)	No special requirements	Encryption required	Encryption required. Storage in secured location is also required when not in use.
Storage on jump or flash drives	No special requirements	Encryption required	Not preferred. However, if this type of media is used, the drive should be password protected and the data encrypted. Should be stored in a secured location when not in use.

Details about how to handle printed student data and transmitting student data can be found at:

- **Handling Printed Student data**
  http://www.purdue.edu/SSTA/datasteward/security/files/Printed.pdf
- **Handling Electronically Transmitted Student Data**
  Pay particular attention the requirements of sending Sensitive and Restricted data by FAX. You should only send that data when the intended recipient can be verified as present when the data is sent, and that you do not leave originals or "transmission confirmation" pages at the machine.
  http://www.purdue.edu/SSTA/datasteward/security/files/Elec%20Trans.pdf

For more information on Purdue's policies for handling Sensitive and Restricted data see the following:

- **Purdue SSN Policy**:
  http://www.purdue.edu/policies/pages/information_technology/v_5_1_print.html
- **Sensitive and Restricted Data Security Video**:
  https://www.purdue.edu/securepurdue/media/SensitiveDataVideo.htm
- **Student Services Security, Data Handling, and Classification Updates**:
  http://www.purdue.edu/SSTA/datasteward/security/updates.php

If you have any questions, please contact the College of Education IT team at edit@purdue.edu. With your help we can keep our students and friends safe and secure Purdue.