Sensitive Data Requests for Student Information
Topics

• General information about Student Data
• Access to Student Data
• Reporting of Student Data
• Responsibilities concerning Sensitive Data
General Information about Student Data

- All student data is governed by privacy laws and policies
- All student data is highly confidential
- All student data is personally identifiable
- Some student data is considered “Sensitive”
- Students control the release of personally identifiable information
- Access to student data is highly controlled
- Some student data is directory information
- Students can restrict release of directory information
Some student data is directory (or public) information - Unless specifically restricted by the student, UCSD considers the following to be public information and can be released without student permission, unless restricted:

- Student name
- Campus/local address
- Campus/local telephone number
- Permanent home address
- Permanent home telephone number
- Date of birth
- College and major
- Dates of attendance
- Degrees and honors received
- Officially recognized activities (not currently maintained on ISIS)
- E-mail addresses
Sensitive Data

**UCSD considers some personally identifiable data as sensitive.** Sensitive personally identifiable information includes:

- Ethnicity
- Social Security Number
- Taxpayer Identification Number
- Most financial information, tax returns, and other information such as Credit Card numbers

Sensitive data is more highly restricted due to its revealing nature and our obligation to protect individual identity. Traditionally, sensitive data has not made available in general access to data. However, in order to have some guidelines and protocols to grant access to sensitive data when required, the following steps have been adopted for consistent application.
Tools, Tables, Warehouse(s)

**TritonLink Tools** *(most of campus uses this)*
- Access to individual student data
- Access to QueryLink – prepared reports, compiled reports
- Access to programs – emailer, class lists

**Data Warehouse Tables**
- Access to student data tables to pull records and compile reports – inquire, secure, restricted, no updating allowed
- Ability to write SQL reports using Data Warehouse tables for input

**Data Marts/Shadow DB or Data Warehouse**
- Secondary access to student data outside the access controlled environment. Owners and users of data marts, shadow systems, and secondary data warehouses are obligated to comply with the data access policies in place for the primary systems.
Takeaways

• All student data is confidential
• All access to student data is controlled
• Sensitive data is highly restricted
• All data providers are responsible for proper access control
• All data bases are subject to access control
Data Policies

Data Policies
• FERPA
• PPM 160-2

Here are some campus and university resource links:

• [http://blink.ucsd.edu/technology/security/personal/](http://blink.ucsd.edu/technology/security/personal/)


• [http://policy.ucop.edu/doc/2710533/PACAOS-130](http://policy.ucop.edu/doc/2710533/PACAOS-130) (Ref: 130.241)