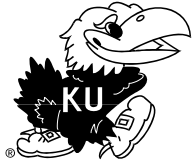


THE UNIVERSITY OF KANSAS



STUDENT INFORMATION SYSTEMS USAGE AGREEMENT

Upon obtaining Student Records Information data in any format, a user is obligated to the following responsibilities:

1. Data provided to you or your department to conduct official university business may be used only for the purpose(s) for which permission has been granted. Any change in use must be preceded by authorization from the data security administrator.

2. Disclosure of personally identifiable information to others without the written consent of the student is prohibited. Departments should be sensitive to the confidential nature of a significant portion of the data received and the legal consequences to a staff member and the University should personally identifiable information be mishandled. Therefore, departments agree not to allow access to data received to any person(s) not authorized for its use.

3. In cases where an administrative officer has been given access for departmental use, that officer is ultimately responsible for the security of the data while they reside in the department. That officer is also responsible for assuring that all individuals who have access to that data within the department are aware of the University policies governing confidentiality.

4. The University uses the statistics generated on the 20th day of classes each semester as the official figures for that semester. Statistical information you may submit on surveys or external reports must reflect the official 20th day figures.

5. Addresses and other directory information of students are basically public information. Directory information is defined as: "information relating to a student: name, current address and telephone number, permanent address and telephone number, e-mail address, level and school, date of birth, major field of study, enrollment status (full-time, half-time, less than half-time), participation in officially recognized activities and sports, height and weight of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational institution attended by the student. The name(s) and address(es) of the student's parent(s) or guardian(s) may be disclosed when used for an official University news release about the student's receipt of

degrees or awards or about participation in officially recognized activities or sports. Such parent information may also be disclosed for purposes of University advancement. The name(s), position(s) and length of service may be disclosed for student employees." Students may request their directory information be withheld from public disclosure. These requests must be honored. Students who have requested their directory information be withheld are easily identified as those having a window shade icon in the upper right of the page on SAKU. On the Student Records Listing of Enrolled Students available through the DEMIS system, choose the field: **FERPA Protection Requested**. Specific University policies and procedures must be followed on the release of all directory information. These policies include procedures for verbal information release, the use of mailing labels and mailing lists, etc. Contact Brian McDow at 864-2017 for policy interpretation.

6. Departments assume the responsibility to maintain a secure environment for any confidential data. This may involve establishing security access procedures to computerized files, keeping disks or printouts in locked cabinets, periodically updating passwords and assuring that terminals are properly signed-off when not in use.

7. The online access codes (sign-ons) provided to approved users are to be utilized by that person only. **DO NOT SHARE SIGN-ONS.** Your access code is confidential.

In addition, the use of downloaded student data is subject to the following regulations:

1. Data files (or their subsets) are for the exclusive use of the authorized KU faculty, staff or student that has been given permission to access the data.

2. If a time limit on the use of the data has been imposed by the data security administrator, then it is the responsibility of the user to destroy all copies of the data file(s) at the designated time, or to obtain an approved extension.

3. Disk, tape, flash drives, or other storage devices containing downloaded data will be kept secure at all times.

Request Form for DEMIS reports: Daily & Census Summary Reports
(Advising Hours Report/Query by specific request; please indicate/explain need for these in job duties box below.)

Name _____

Online ID _____

Department _____

Campus
Address: _____

Address line 2: _____

Email Address: _____

Job Title (please list your working job title): _____

Please list the job duties which require this access, and indicate the purpose for which data from DEMIS will be used:

Please indicate the programs or plans you wish to access. _____

I have read and understand the attached Student Records Information Systems Usage Agreement. I have retained a copy for my reference. I agree to comply with it.

User Signature: _____ Date: ____/____/____

I approve system access for this employee.

Department Head Signature: _____ Date: ____/____/____