Executive Sponsor:
Provost & Senior Vice-President
for Academic Affairs

Responsible Office(s):
Institutional Research Office
Registrar's Office

Approved: May 2018
Revised: n/a

STUDENT DATA RELEASE POLICY

I. POLICY STATEMENT

This policy sets forth the conditions under which student data may be distributed internally or externally in a manner consistent with The Family Educational Rights and Privacy Act (FERPA) and University policies, as listed below. A procedures attachment is also provided.

II. REASON FOR POLICY

This policy defines how University of Scranton student data is released to faculty, staff, and other third parties. The purpose of this policy is to guide the data steward, as well as the data requestor.

Definitions of student data (aggregate, directory, individual, official, and operational) are included in this policy for uniformity purposes.

Policy procedures (attachment) covers five (5) areas of data release: procuring, utilizing, distributing, securing, and properly disposing of data.

III. ENTITIES AFFECTED BY THIS POLICY

Staff, faculty, and other parties requesting data; also departments and staff who fulfill requests for student data.

IV. WEBSITE ADDRESS FOR THIS POLICY

This policy can be found at the following locations on the web:

http://www.scranton.edu/academics/provost/academic_policies.shtml

V. RELATED DOCUMENTS, FORMS, AND TOOLS

- *Data Standards Manual*
    - *https://www.scranton.edu/information-technology/services/banner.shtml*
- *Institutional Review Board for the Protection of Human Subjects (IRB)*
    - *http://www.scranton.edu/academics/provost/research/sub%20pages/IRB.shtml*
- *Family Educational Rights and Privacy Act (FERPA)*
    - The University of Scranton recognizes the privacy rights of individuals who are or who have been students, as guaranteed by the Family Educational Rights and Privacy Act (FERPA) of 1974. To review the University's FERPA policy, refer to the latest undergraduate catalog at:
    - *http://www.scranton.edu/academics/registrar/university-catalogs.shtml*
- *Records Management and Retention Policy*
    - *http://www.scranton.edu/general-counsel/policies.shtml*
- *Information Technology, Information Management & Security Policies*
    - *http://www.scranton.edu/information-technology/policies.shtml*

VI. CONTACTS

For policy clarification and interpretation contact: the Institutional Research Office at 570-941-7693 or email institutionalresearch@scranton.edu, or the Office of the Registrar & Academic Services at 570-941-7721.

VII. DEFINITIONS

Student Data
Student data is defined as any information about an individual student or group of students collected and maintained by the University, including, but not limited to, personally identifiable information, demographic, registration, academic history, discipline, and/or other student-related data. Data is collected for official University business.

Aggregate Student Data
Aggregate data is defined as summarized data that excludes identifying information such as student names and/or Royal IDs (R#). Any aggregated data cell with a value less than 10 should not be included in a published report, unless required by an authorized government agency, including accreditors, or approved by the relevant data steward.

Directory Data
The University considers the following to be public information which may be made available, at its discretion, without prior consent of the student, unless the student requests his/her information is kept confidential, per FERPA regulations and University policy:

- Name
- Former Name(s)
- Address (local and permanent)
- Telephone Number (campus/local and permanent)
- Date and Place of Birth/Age
- Photograph
- Major Field of Study
- Participation in Officially Recognized Activities and Sports

- Weight and Height of Members of Athletic Teams
- Email Address
- Dates of Attendance
- Enrollment Status
- Campus Employment
- Class Level
- Expected/Actual Date of Graduation
- Degrees, Awards, Academic Honors

Individual Student Data
Individual student data can only be released in a manner consistent with FERPA, its implementing regulations and university policy.

Official (Census) Student Data
The Institutional Research Office reports the official fall and end-of-term(s) enrollment; graduation; and, retention and graduation rates data. Official data is to be used for accreditation purposes, external surveys and reporting, and other legitimate business needs. Official data is reported to the federal (i.e. IPEDS) and state government, and is considered the 'Data of Record' for the University. Official data is released to the University community at several points throughout the academic year.

Operational (Live) Student Data

Offices are often asked for student data from the current date in order to perform departmental operations. This data may or may not be the same as the official data since official data is extracted (frozen) on established census dates.

Data Steward
University officials, or their designated representatives with decision-making authority, responsible for data handling practices in their divisions.

VIII. RESPONSIBILITIES

- Persons requesting student data are expected to complete a student data request per the accompanying 'Procedures' section of this policy.

- Data Stewards, or those acting on behalf of the University, including third-party contractors, are expected to approve/deny requests for student data per the accompanying 'Procedures' section of this policy.

IX. PROCEDURES

Policy procedures cover five (5) areas of data release: *procuring, utilizing, distributing, securing, and properly disposing of data.*

Procuring

1. To obtain student data, faculty and staff should complete the Student Data Release Request Form. Requests for student data will be fulfilled through the following areas and data stewards; Institutional Research or the Registrar will route requests to appropriate areas if needed:

   Individual student(s) demographic, academic record, master schedule, or course enrollment data – Registrar & Academic Services

   Aggregate or Official student data (enrollment, graduation, retention, or survey results) – Institutional Research

   Admissions Data (applicants, admitted, confirmed) – Admissions & Enrollment

   Campus Life Data (residence life, clubs/organizations, career development) – Student Formation & Campus Life

   Student Financial Data – Financial Aid, Comptroller

Restricted data will be released in accordance with the University's **Information Classification Policy**.

Student financial data will be released, except where prohibited by federal Department of Education policy,

2. Requests for student data are evaluated on a case-by-case basis. The timeliness of the review will vary depending on the complexity of the request and the approvals needed.

   Requests are approved or denied according to the following:

   - Academic Departments/Units, Faculty Committees, Faculty Members

     Faculty members, with a legitimate educational interest in the data, may request data for students who they are instructing or advising. Academic Department Chairs may request student data for students enrolled in programs offered by their department. Requests for data on students enrolled in other academic departments need approval from the Dean's Office(s) Data Steward. Requests for University-wide student data need approval from the Provost's Office Data Steward.

   - Research Purposes

     Student data may be provided to researchers affiliated with the University of Scranton. The researcher must submit proof of University of Scranton Internal Review Board (IRB) approval or waiver when making a request for student data to be used in scholarly

research. Additionally, the request must have appropriate approval as outlined above. For student researchers, authorization by the researcher's faculty advisor at the University of Scranton is required, as well as the appropriate approval as outlined above for Academic Departments.

- Administrative Departments/Units, Committees, Staff Members

  Student data may be provided to other University school officials with a legitimate educational interest in the data requested. The department supervisor, data steward, or their designees must authorize these requests. For purposes of this section, University school officials are university employees with a general or specific responsibility for promoting the educational objectives of the University or third parties under contract with the University performing the same function that a University school official would otherwise perform. A legitimate educational interest is defined as the need to review or obtain an education record in order to fulfill a school official's professional responsibility. The need to know must be related to the school official's job responsibilities.

- Student Organizations

  Student contact data may be provided to moderators of student organizations at the University of Scranton with the proper approvals, as outlined above for Administrative Departments.

- Third-Party Contractors/Vendor Organizations/Consortiums

  Third-party contractors, vendor organizations, and consortiums to whom the University has outsourced institutional services or functions that involve access to student data must agree to adhere to FERPA regulations and university policy regarding collection, use, maintenance and disposal of student data. Requests from third-parties take the form of contracts or other service agreements and are not processed using the Student Data Release Request Form.

- Authorized Government Agencies

  Student Data may be provided to authorized representative of the Comptroller General of the U.S., the Attorney General of the U.S., the U.S. Secretary of Education, and state and local educational authorities, but only in connection with the audit or evaluation of federally supported educational programs, or in connection with the enforcement of, or compliance with, federal legal requirements relating to these programs, or specifically required to be reported by state or federal law. These officials will protect information received so as not to permit personal identification of students to outsiders, and the data shall be destroyed when no longer needed for the purposes above. Requests from government agencies for mandated compliance reporting completed by an operational unit of the University are not processed using the Student Data Release Request Form.

- Media and Mass Email

  The media, including campus publications, must contact Office of Media Relations (570-941-7662) when requesting student data.

  Requests for mass email services to students' University email accounts are governed by the *Policy for Distributing Broadcast Email*, found with Information Technology Policies referenced in Section V.

Utilizing

Data must be used for the legitimate educational purposes(s) for which it was requested and must be kept confidential, unless specified in the request form.

Student data is provided upon request for compliance purposes and/or use in institutional analysis. Reports of student data may not be reproduced, published, publicly posted, or used for any secondary purpose without obtaining permission from the office that originally provided the data.

Please see the University's **Information Access Policy**, found with Information Technology Policies in Section V.

Distributing

Distribution of data refers to University of Scranton student data in any format, including hard copy or electronic format.

All student data are released for use by the requesting department only. Authorized individuals and their designees (including contracted vendors) must agree to use the data provided for the purpose specified in the request and, unless required and authorized, must agree that data obtained will not be reproduced, published, publicly posted, shared, or used for any secondary purpose.

Misuse of student data may subject requestors or their designees to civil and/or criminal penalties and/or university discipline. To ensure compliance, all elements of the intended data uses must be stipulated in the data request.

Securing

All student data released pursuant to this policy is confidential information; must be protected from loss, theft, copying, redistribution or disclosure; and must be handled so as not to cause a breach of the confidential nature of the information.

Please see the University's **Information Security Policy** for guidance on securing University data, found with Information Technology Policies in Section V.

Disposing

Information released pursuant to this policy and any copies of such information must be destroyed when no longer needed for the purpose for which it was originally requested except as required by federal or state law or regulation, or University policy.

Please see the University's **Records Management and Retention Policy** referenced in Section V for guidance on the disposal of data. Please note that some student data may need to be retained on an alternate schedule per accreditation standards (see individual department accreditation standards).