Oklahoma State Regents for Higher Education

Data Access and Management Policy

Purpose
This policy establishes the principles governing access to and the dissemination of information gathered and maintained through the Oklahoma State Regents for Higher Education (State Regents) unitary data system.

Scope and Applicability
This policy shall apply to all data and information products created, collected and maintained by or for the State Regents data system, whether in electronic, paper or other format. When access to information, as it is collected or maintained, is restricted by federal or state laws for confidentiality, privacy, or other authorized purpose, the information shall be processed (e.g., aggregated, summarized or characterized) as appropriate to provide access while meeting the requirements for restriction. This policy will adhere to restrictions on the releases of confidential information identified in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and its implementing regulations found in Title 34 C.F.R. Part 99, which established restrictions and penalties for the improper release of information contained within a student record.

Background
The State Regents manage a unit record database containing public and private higher education institutional data submissions which are used by the State Regents for state and federal reporting, policy analysis, and decision-making.

The unitary data system contains four files:
(1) Student Enrollment File,
(2) Student Course Enrollment File,
(3) Class File, and
(4) Professional Staff File.

While each of the four files are collected and stored separately, the usefulness of the entire unitary data system is in the ability to connect data across files to generate complex data sets. These files also can be integrated with other data sets, such as K-12 and employment information.

The System Research Division of the State Regents protects the unitary data system in accordance with FERPA. Because the data system contains individual data on students and staff, this policy is subject to both privacy and confidentiality procedures.

Definitions
Confidentiality consists of how personally identifiable information collected by an authorized agency is protected and when consent by the individual is required. FERPA guards the confidentiality and access to certain educational records, but not to personnel data. To protect

confidentiality and privacy of individual records, the individual record is subject to restricted access defined in this policy and to summative reports.

Privacy is the right of individuals to have the information about themselves adequately protected to avoid the potential for substantial harm, embarrassment, inconvenience, or unfairness.

Education records means those records directly related to a student and maintained by an educational agency or institution.

Personally identifiable information consists of information contained in an education record such as a personal identifier, characteristic, or other information that would make the students identity easily traceable.

Directory information consists of information contained in an education record which would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to the students date and place of birth, field of study, dates of attendance, degrees and awards received.

Research is a formal investigation designed to develop or contribute to generalized knowledge.

Legitimate educational interest, for purposes of this policy, is an endeavor meant to further the understanding of educational practices, methods, and/or theory that is expected to be analyzed through formal, accepted research practice and the results of which, consistent with FERPA, will be disseminated in such a manner as to benefit the educational community and/or public in general.

Policy

Data collected and maintained in the State Regents' data system shall be managed in a manner which will promote access to and dissemination of information that improves the education-related decisions of parents, teachers, administrators, policymakers, and educational stakeholders as well as the general public.

This policy articulates three privacy and confidentiality protections:

(1) **Security** includes the measures in place to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers, it is essential that there be a high level of protection that provides integrity and availability commensurate with the level of risk and magnitude of harm.

(2) **Access** to the data is restricted by the State Regents and significantly limits who can view the data and for what purposes. There are five access levels, each of which is consistent with a specific educational purpose as defined in Section 99.2 of the FERPA regulations.

(3) **Disclosure** in summary reports is designed to protect individual data. In cases where populations include only a few individuals, no group smaller than six individuals is reported.

Access Level
Access levels are assigned to maximize public usage without risking disclosure of personally identifiable information.

Level 1 allows authorized State Regents' staff to read and write to all records and fields in the database. This access level is only permitted to a minimum number of authorized staff members who operate or manage the data system or are responsible for maintaining the accuracy and security in the performance of their duties.

Level 2 allows researchers, education groups, and other parties who express legitimate educational interests to read all records and fields in the database to further the understanding of educational practices, methods, or theory that would be expected through acceptable research practice.

Level 3 allows personally identifiable information plus those data that are considered directory information only.

Level 4 allows individual records without personally identifiable information.

Level 5 allows summaries of data only. The State Regents will block any aggregate results when fewer than six students or educational personnel might be disclosed.

Disclosure of Data
Private or confidential data on an individual shall not be created, collected, stored, used, maintained, or disseminated by the State Regents in violation of federal or state law and shall not be used for any purpose other than those stated. If the State Regents enter into a contract with a private person or third party to perform any State Regents' functions, that agreement shall require that the data be protected in the same fashion.

Under this policy, no private or confidential data will be released except under the following circumstances as stated in Section 99 of the FERPA regulations:

1. To staff of the higher education institutions who have released the data to State Regents when the determination has been made that there are legitimate educational interests, under Section 99.36(b)(2).

2. To comply with a subpoena or court order, under Section 99.31(a)(9)(A).

3. To honor a request from a judicial order, or an authorized law enforcement unit, or lawfully issued subpoena, under Section 99.31(a)(9)(i). A law enforcement unit refers to all state and local prosecution authorities, all state and local law enforcement agencies, the Department of Corrections, and probation officers who are part of the Judiciary.

4. To educational officials in connection with an audit or evaluation of a federal or state supported education program, under Section 99.32(c)(3).

5. To appropriate parties in connection with an emergency if such knowledge is necessary to protect the health and safety of the student or other individuals, under Section 99.36(a). In cases of health or safety emergency, the request for release must first be directed to the school district that owns the data. The Director, under Section 99.36(a), may also convene a committee to evaluate the request to determine whether or not the person who would receive the information is in a position to deal with the emergency and the extent to which time is of the essence.

6. To research proposals approved by the Chancellor or designee, when a requestor demonstrates a clear legitimate educational interest, provided that personally identifiable information if discovered is not disclosed to anyone other than the initiator of the request. At the discretion of the Chancellor or designee, any request may be denied.

Data will be disclosed only on the conditions that (1) the party to whom the data are released does not disclose the information to any third party, (2) the data are protected in a manner that does not permit the personal identification of an individual, (3) the data are used solely for the purpose requested, and (4) the data are destroyed when no longer needed for the purposes under which the disclosure was granted.

If it is determined that personally identifiable information was disclosed in violation of this policy, all parties will not have access to any State Regents' data for five years. In addition, all violations will be reported to the appropriate federal and state enforcement agencies. The Privacy Act of 1974 states that disclosure of individually identifiable information in any manner to any person or agency not entitled to it shall be guilty of a misdemeanor and fined not more than $5,000.

State Regents will account for all disclosures. This includes the date, nature, and purpose of the disclosure, and to whom the disclosure was made. Data access provisions may change at the discretion of the State Regents or if mandated by federal statue, state law, or administrative rules.

Requirements for Security, Privacy, and Confidentiality

Commercial use of data obtained under such a request is prohibited. Recipients **do not** attain ownership of the data. Such data may not be shared or distributed, and all copies must be destroyed when the researcher completes the analysis or report. Data, copies of data, and all reports must be maintained in a secure environment to prevent unauthorized access. A secure environment includes any electronic media, personal computer, server, or network on which the data reside. Compliance with these security requirements may be monitored by unannounced, unscheduled inspections of the data user's work site by State Regents' staff or designated representatives.

All users of the requested data must sign the Data Request Form that explains how the data are to be stored, used, maintained, and disseminated. When the Chancellor or his designee approves a research proposal request pursuant to this policy, requestor shall be required to forward a copy of

any analysis or reports created with the State Regents' data system to the System Research Division of the State Regents.

Requests for Data Access

Pursuant to the State Regents' Data Access and Management Policy, researchers, education groups, and other parties who express legitimate education interests in the data, as defined in this policy and consistent with FERPA, may submit requests for access to State Regents' data system. In reviewing requests for data, consideration is given to access permitted by statute, federal law, privacy concerns, security procedures, availability of staff to monitor the data release, and the perceived benefits of the research. Entities seeking access to the State Regents' data system are required to submit a Data Request Form stating how the data will be used, and a description of the data needed. Release of data is subject to approval by and at the discretion of the Chancellor or designee.

Upon request of individuals under Section 552a(f)(1) of the Privacy Act of 1974 or Section 99.20 of FERPA to gain access to their records contained in the State Regents' data system, State Regents will provide a copy of all or any portion in a comprehensible form and will consider requests to amend the record.

Processing Request

Completed requests will be reviewed and a response provided in an appropriate manner. In the event a request is rejected, specific reasons shall be given and if appropriate, may include information concerning possible alternatives. Requests may be rejected if information on the application form is incomplete.