3344-8-02 Administrative data policy.

(A) Purpose

(1) Information maintained by Cleveland state university is a vital asset that shall be available to all employees who have a legitimate need for it.

(b) Private information

Private information is data that the data trustees judge to require special procedures for access. Private information may be subject to disclosure under the Public Records Act and is made available to a select group of Cleveland state employees based on their job function. Private information is broadly defined as that which should be reasonably protected from disclosure. For example:

(i) Data not specifically protected by statute, regulation, or other legal obligation or mandate.

(ii) Shall be protected due to contractual, ethical, or privacy considerations.

(iii) Access, disclosure, or modification could cause financial loss or damage to CSU s reputation.

(iv) Examples (not all-encompassing)

(a) Directory information of students who have not requested FERPA privacy inclusion

(b) Instructional information such as tests, quizzes, and course shells in a learning management system (LMS)

(c) Proprietary information used to run the business of the university

(d) Email (generally)

(c) Public information

Public information is all data that is neither restricted, nor judged by data trustees to be sensitive

or private. The accessible data volume should be as great as possible to enable those who need the information to have access. Data should be part of an open atmosphere and readily available. Public information is subject to disclosure to all Cleveland state employees as well as the general public under the Public Records Act. Public information is broadly defined as that which is intentionally displayed for anyone to use, including:

(i) Disclosure is routine and/or deliberate.

(ii) Can be subject to use restrictions (copyright) but no harm done in disclosure.

(iii) Data that is public by law is subject to review before disclosure by the office of general counsel.

(d) Protection of data

(i) Users shall comply with all reasonable protection and control procedures for administrative data to which they have been granted access. Sensitive and private data can never be stored on departmental computers or servers, cd s, thumb drives or any easily transportable medium. All sensitive data shall be stored on secured storage located within the university s data center.

(ii) It is never acceptable to store sensitive data such as grades, social security numbers, correspondence between student and faculty, classified research, etc., on externally hosted systems, including cloud-based storage systems (includes, but is not limited to, services such as dropbox, google drive, and microsoft onedrive), without a contract that

director of admissions) who oversee the capture, maintenance, and dissemination of data for a particular operation. Data custodians are responsible for making security decisions regarding access to the data under their charge.

(c) Data users are individuals who access university data in order to perform their assigned duties or to fulfill their role in the university community. Data users are responsible for protecting their access privileges and for proper use of the university data they access.

(4) Responsibilities of data trustees, data custodians, and information services and technology

(a) Criteria for determining access

(i) Data custodians are ultimately responsible for assigning access to all types of data on an individual basis; however, general criteria for determining access to both sensitive and private information include the following:

(ii) Human resources/payroll data can be made available as follows:

(a) Personnel in the employee s supervisory chain of authority

(b) Human resources, payroll, and business contacts in departments shall have access to human resources/payroll data for employees in their departments.

(c) Authorized employees of the department of human resources, payroll department, budget office, controller s office, grant accounting, department of audits, the office of

general counsel, the office for institutional equity, and the department of law enforcement and safety, shall have access to human resources/payroll data on a case-by-

(c) Authorized employees of business and finance, office of general counsel, division of law enforcement and safety and the department of audits who have a business need to access the data

(iv) Student data can be made available as follows:

(a) To school officials with legitimate educational interests. A school official is a person employed by the university in an administrative, supervisory, academic or research, or support staff position; a person or company with whom the university has contracted (such as an attorney, auditor, or collection agent); a person serving on the board of trustees; or a student serving on an official

States, state education authorities, organizations conducting studies for or on behalf of the university, and accrediting organizations;

(d) In connection with a student s application for, or receipt of, financial aid;

(e) To comply with a judicial order or lawfully issued subpoena;

(f) To parents of dependent students as defined by section 152 of the Internal Revenue Code;

(g) To appropriate parties in a health or safety emergency;

(b) Development of access policies and procedures

Each data custodian shall be individually responsible for establishing data access procedures that are unique to a specific information resource or set of data elements.

(c) Promotion of accurate interpretation and responsible use

(i) Data trustees shall develop policy to promote the accurate interpretation and responsible use of administrative data.

(ii) Data custodians are responsible for making known the rules and conditions that could affect the accurate presentation of data. Persons who access data are responsible for the accurate presentation of that data.

(iii) Data custodians shall support users in the use and interpretation of administrative data,

3344-8-02

department within the university or leave employment of the university.

Policy Name: Administrative Data Policy.
Policy Number: 3344-8-02
Board Approved: 5/20/2015
Effective: 6/01/2015