Data Stewardship:

Procedure for Data Access to Banner Student Module

This procedure defines the ways in which Lane Community College will grant data access requests for Lane Community College employees. It outlines the process an employee will follow to ensure proper training and level of access is issued.

Legitimate Educational Interest is the demonstrated "need to know" by those school officials of an institution who act in students' educational interests.

A school official is:

- A person employed by the college in an administrative, supervisory, academic, research, or support staff position;
- A person elected to the Lane Community College Board of Education; or
- A person employed by or under contract to the college to perform a special task such as the attorney or auditor.

A school official has legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for Lane Community College. Those responsibilities include:

- Performing a task that is specified in his or her position description or by a contract agreement;
- Performing a task related to a student's education;
- Performing a task related to the disposition of a student; or
- Providing a service or benefit relating to the student or student's family, such as health care, counseling, job placement or financial aid.

Lane classifies its data based on sensitivity level and further defines legitimate educational interest through this classification of data. Some data has limited access and is not meant for general distribution. Limited access data is confidential and only accessed through the appropriately designated functional areas that have a "need to know" for this data.

Classification of Data

Restricted - Data that are of a sensitive or highly confidential nature and are restricted from general distribution. Special authorization must be approved before access or limited access is granted. (Examples include social security numbers, counseling records, protected health information).

Internal Sensitive - Data that are only available to staff with the required access in order to perform their assigned duties. (Examples include individual student educational records used for federal and state reporting).

Internal General - Data used for college activities and outreach, but not for external distribution unless otherwise authorized. (Examples include aggregate data for program review, contact lists by program of study) This is the classification of access that will be granted to the majority of staff and faculty.

Local - Data that are captured by various Lane units, are not integrated or accessible to the enterprise systems but that are needed to support the work of particular units.

Third-Party Integration Systems such as SARS, International, Health Clinic, Lumens, and ProClass

Satellite Databases such as Health Professions Applications.

Public - Data that are openly available to all faculty, staff, students and the general public. (Examples include course schedules, public web pages, and press releases.)

Operational – internal data used to support analysis and decision making. These data are imperfect but effective, dynamic, actionable, and clearly defined and understood.

Official – external data used for accountability and communications

Accessing College Data

To help prevent unauthorized access, there is a need to clearly define those who can view, access and responsibly use each level of data. Preventing unauthorized access involves many other safeguards, but knowing who is (and is not) authorized is fundamental.

Users of institutional data must:

- Access data only in conducting college business, and in ways consistent with furthering the college mission.
- Respect the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to the data to which they have access.
- Abide by applicable laws, regulations, standards, and policies with respect to access, use, disclosure, retention, and/or disposal of information.
- Complete college approved training, data access requests and FERPA and confidentiality statements.
- Users of institutional data must not:
    - Disclose data to others except as required by their job responsibilities.
    - Use data for their own or others' personal gain or profit.
    - Access data to satisfy personal curiosity.

Access Approval

- Complete mandatory annual FERPA training through the Safe Colleges Human Resources module: https://lanecc-or.safecolleges.com/training/assignments
- Complete mandatory annual Implicit Bias training through the Safe Colleges Social and Behavioral module: https://lanecc-or.safecolleges.com/training/assignments
- Review and acknowledge read receipt of "How to Practice FERPA"

Access Request

In general, contact lists for student outreach will be made available and will contain the following information as determined by the college: Name, L#, LaneCC.edu email address, phone number, mailing address, program of study. All other data requests must follow the appropriate access request procedure.

- Complete the appropriate access request form.
    - o Data Request Form
        - ▪ IR determines if this will be an Argos Report or a Non-Standard Report from IR
    - o Banner Student Module Request based on job
- Banner and ARGOS training as needed
- FERPA and Confidentiality Statements on file with Human Resources

Continued Access

- Review of job description and legitimate educational interest based on job requirements
- Current with FERPA and Implicit Bias training
    - o This includes no record of reported FERPA violations
- Review of signed FERPA and confidentiality statements on file with Human Resources