

## Protocols for Processing Owl Life Community Access Requests

### 1. Purpose

This document outlines the requirements and considerations for granting and revoking request for Community Access to the Campus Labs Engage (branded locally as Owl Life) system submitted to Strategic Planning, Assessment, and Analysis (SPAA).

### 2. Background

The Division of Student Affairs has been entrusted with access to sensitive student-level institutional data, accessible via the Campus Labs Engage platform. As such, the Division of Student Affairs has developed protocols through which access to that data is reviewed and approved.

### 3. Scope

These protocols apply to Division of Student Affairs' staff requesting Community Access to the Campus Labs Engage (Owl Life) system.

### 4. Definitions

- a. *Owl Life (Campus Labs Engage)*: Software used in the collection and management of student engagement and institutional data that is pertinent to work within the Division of Student Affairs. Campus Labs Engage is branded at KSU as Owl Life.
- b. *Community Access*: Denotes users who have access to administrative tools within the Campus Labs Engage (Owl Life) system that extend beyond the management of a single department's or organization's page/account within the system. Community Access is granted to provide appropriate access based on a user's job function. Community Access is available at the following levels:
  - i. *Full*: Users who have administrative permissions over the entire Owl Life system, including the ability to generate and view data that contains sensitive user information, approve all types of requests and submissions, and create, change, or delete any content in the community.
  - ii. *Branch*: Users who have the ability to approve all types of requests and submissions, and create, change, or delete any content within a Branch for which they have been given access.
  - iii. *Limited*: Departmental-Level Users who have access to a specified set of administrative tools based on a business need. This level of access may or may not include the ability to generate and view data that contains sensitive user information, depending on the administrative tools to which the user is granted access.

Note: A glossary of Owl Life terminology may be found on the SPAA website, accessible at [studentaffairs.kennesaw.edu/assessment](http://studentaffairs.kennesaw.edu/assessment).

- c. *Institutional Data*: Those data, regardless of format, maintained by Kennesaw State University (KSU) or a party acting on behalf of KSU for reference or use by multiple University units. Institutional Data currently accessible via the Community Access to the Campus Labs Engage (Owl Life) system:

- i. Demographic Data: name, sex, birthdate, citizenship status, commuter status, university affiliation
  - ii. Contact Information: address, KSU email address
  - iii. Academic Performance: cumulative institutional GPA, enrollment status
  - iv. Academic Details: class standing, major, matriculation term, previous term enrolled, transfer status, athlete status
- d. *Least Privilege*: A principle in which users are given the minimal degree of access and/or permissions necessary to complete a legitimate business and/or academic purpose.

## 5. Protocol

Strategic Planning, Assessment, and Analysis (SPAA), under the direction of the Senior Associate Vice President of Student Affairs, has been charged with administering and maintaining Community Access user permissions on behalf of the Division of Student Affairs.

- a. Requests for Community Access shall be submitted via an online form accessible via the SPAA website. Each request submitted to SPAA will be reviewed in consideration of the following:
  - i. Alignment between the expressed purpose for Community Access and departmental mission;
  - ii. Alignment between the expressed purpose for Community Access and job function; and
  - iii. Alignment between the level of Community Access requested and the expressed purpose for Community Access, in accordance with the principle of least privilege.
  - iv. Approval of Community Access request by the requester's supervisor and senior leadership member.
- b. Upon completing the review, Community Access request may be approved, denied, or returned to the requester for modification. In cases where access is approved, fulfillment of the Community Access request will be completed after the following conditions have been met:
  - i. Successful completion of training by the user covering information relevant to the level of Community Access for which they will be provisioned; and
  - ii. Successful review of the user's compliance with University data security policies, certifications, and training.

## 6. Enforcement and Implementation

- a. SPAA shall be entrusted with the implementation, review, and enforcement of these protocols.
- b. Periodic review of Community Access levels shall be conducted by SPAA on an on-going and regular basis to ensure current Community Access permissions are up-to-date and reflective of current business needs.
- c. SPAA, under the authority of DSA Senior Leadership, reserves the right to temporarily rescind the Community Access of a user if it becomes aware of a potential breach of any provision of this document has taken place and initiate an access review process, as outlined in the Owl Life Community Access Suspension and Review Process document.
- d. SPAA is responsible for ensuring users with Community Access permissions have been provided with training, support, and resources necessary to maintain compliance with these protocols.

## 7. Exceptions

Exceptions to the provisions established in these protocols may be granted in cases where lack of access would interfere with legitimate academic or business needs.

**8. Associated University Policies**

Policies are available via the KSU Policy Portal at [policy.kennesaw.edu](http://policy.kennesaw.edu)

- a. Data Security Policy
- b. Information Technology Acceptable Use Policy
- c. Enterprise Information Security Policy