KENNESAW STATE UNIVERSITY
DIVISION OF STUDENT AFFAIRS

Standards of Use of Owl Life Community Access Users

1. **Purpose**
   This document outlines the standards applicable to users provided Community Access within the Campus Labs Engage (branded locally as Owl Life) system.

2. **Background**
   The Division of Student Affairs has been entrusted with access to sensitive student-level institutional data, accessible via Owl Life. As such, the Division of Student Affairs has developed standards to which users provided with Community Access to the Owl Life platform must adhere in order to maintain their access level.

3. **Scope**
   These standards apply to Division of Student Affairs' staff provided with Community Access to the Owl Life platform.

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, branded at KSU as Owl Life.
   b. *Community Access*: Denotes users who have access to administrative tools within the Owl Life system that extend beyond the management of a single department's or organization's account within the system. Community Access is scaled to meet the specific needs of a user in order to restrict the unwarranted access to sensitive user data and system settings. 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.
   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 obtaining Community Access permissions within the Owl Life platform:

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. Standards

a. Community Access Users:
   i. Users provided with Community Access are responsible for implementing, reviewing, and monitoring internal policies, practices, etc. to ensure compliance with these protocols, University data security policies, and FERPA regulations.
   ii. Only users provided with Community Access shall access institutional data stored in the Campus Labs Engage platform. Community Access users shall not distribute institutional data beyond those entities identified in their original request for Community Access.
   iii. Users with Community Access shall make use of permissions granted and access data in a manner that is consistent with the expressed business purpose included in the original request submitted to Strategic Planning, Assessment, and Analysis (SPAA).
   iv. Community Access users acknowledge that access to systems and data is a privilege and that the user will act responsibly when granted system permissions and access to data for which they have permissions, including respecting the privacy of members of the university community. Community Access users must maintain the confidentiality of data in accordance with all applicable laws, KSU privacy policies, and data security standards.
   v. Community Access permissions do not imply authorization for copying, further dissemination of data, or any use other than the use for which the user was originally authorized.
   vi. Community Access users shall participate in Owl Life Community Access training on at least an annual basis in order to maintain their access level.

b. Supervisors of Community Access Users:
   i. Supervisors of users provided with Community Access are responsible for notifying SPAA of significant changes to the user's job function or employment status that may alter their need for Community Access.
   ii. Supervisors of users provided with Community Access are responsible for ensuring the staff they supervise maintain compliance with these protocols, University data security policies, and FERPA regulations.

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

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