

POLICIES AND PROCEDURES

[User Accounts](#) | [Course Data](#) | [Email](#) | [Group Portal](#) | [Targeted Announcements](#) | [Data Privacy](#) | [Acceptable Use](#) | [Student Computing Practices](#) |

Purpose

The purpose of this document is to establish internal processes and procedures for the Campus Connect web portal. When completed, this document will be posted on Infonet and the Campus Connect project website.

User Accounts

1. Procedure for new student, faculty and staff accounts:
 - Students get a ZK record (user ID) when their admissions application is accepted.
 - Work study students will receive an employee role via LUM screen in HRS.
 - Staff and faculty (excluding non-employees) get a ZK record (user ID) when they are entered into HRS on the LUM screen with a PIN.
 - Temporary employee user ID's (ZK record) will be set up manually by Information Security according to the prescribed naming convention.
 - Existing staff members will be "grandfathered" into the portal with their current email addresses and display names.
 - The user ID (ZK record) and email address for new employees is based on their legal name as entered in HRS.
 - Staff members who have a number in their user ID may request an email alias through CO-Information Security by submitting a Help Desk ticket.
2. Procedure for user ID (ZK record) changes:
 - Information Security will process user ID changes for students, faculty and staff.
 - Student name changes must first be processed by the Registrar. Then the student must submit a Help Desk ticket to request a user ID change.
 - Staff and faculty name changes must first be processed by HR. Then the staff or faculty must submit a Help Desk ticket to request a user ID change. Faculty name changes must also be updated in SIS via a nightly batch job
3. Procedure for user purges and role maintenance:
 - Student accounts will be purged (deleted) from Campus Connect (not the ZK file) when they meet the following two conditions:
 1. Never logged in to the portal
 2. Not enrolled in the past six terms
 - Student accounts that have a faculty or employee role will not be purged, however the student role will be removed by blanking out the PIN field on screen 103 in SIS.
 - For Faculty accounts, the faculty role will be removed from Campus Connect when they have not taught for three semesters. This will be accomplished by a batch job to remove the PIN from screen 1F3 on SIS which will in turn generate LDI events to remove the faculty role in Campus Connect. A listing of these faculty accounts will then be checked in HRS to see if they have an active assignment. If they do not, a batch job will remove the PIN from their LUM screen, thus removing the employee role.
 - Staff accounts will be deleted when the PIN is removed from the LUM screen in HRS by HR Staff. If the staff account also has a student or faculty role the account will be preserved but the employee role will be removed.
 - For all institution roles (student, faculty, staff), the Campus Connect account will be disabled once there is no institution role in the ZK record (user ID).
4. Procedure for suspected fraudulent activity:
 - Any reports of suspected fraudulent activity must be reported to Information Security immediately. Information Security will set a "admin disabled" flag on the user account so that it cannot be edited except by Security staff. The user will not be able to log in to Campus Connect if the "admin disabled" flag has been set. If they attempt to login they will receive a page that says "Your account has been disabled. Please contact the SOS Help

-
- Desk". The SOS Help Desk will forward users to Information Security.
5. Procedure for password resets:
 - Regional staff will not have access to reset passwords through the admin GUI. Staff can use the self-service tools for user ID look-up and password resets to assist users.
 - The SOS Help Desk will have access to reset passwords for students, faculty and employees through the admin GUI. Before a password can be reset, the Help Desk must obtain the user's name, birth-date, last four digits of SSN and zip code to confirm their identity.

Course Data:

1. Procedure for course loads:
 - Summer and fall courses will be loaded immediately after spring 10-day count.
 - Spring courses will be loaded immediately after fall 10-day count.
2. Procedure for course purges:
 - Courses will be purged from Campus Connect immediately after EOT for each term.
(Note: This does not purge courses from the eLearning system)

Email Policies & Procedures (when accessing through Campus Connect):

1. Account quotas:
 - Staff and faculty receive a minimum of 50MB
 - Students receive a minimum of 15MB
 - All users can increase their quota via a self-service tool
2. File size limits:
 - Files cannot exceed 10MB. There is no limit to the number of files that can be attached to an email.
3. Auto-forwarding college email
 - Users cannot auto-forward their college email to any external email system.

Group Portal Procedures:

1. The Group Portal allows students, faculty and staff to create and manage homepages for clubs or other affiliations and interests through the Campus Connect portal. Groups will fall into two categories: public and restricted. Public groups are open for any Campus Connect users to join. Restricted groups are subject to certain membership criteria. For example, to access a group home page for a college sanctioned group such as SGA, an individual must first be accepted as a member of that organization. Each group page contains the following tools: message board, chat, link publishing, news publishing, photo publishing, email, file sharing, calendar and announcements. Any Campus Connect user can request the creation of a group homepage by filling out the application on the "Request Group" tab within the Group Portal.
2. Requests for new groups will be reviewed weekly by the group administrator or designee.
3. The group administrator will respond to every request. All group requests will be approved as long as they meet the standards set forth by the "Groups Policy". If the group is approved the group administrator will email instructions for building their new group page to the group leader. If the group is denied the user will receive a short explanation of why it was denied, including a link to the "Groups Policy" if necessary.
4. Neither the group administrator nor any other representative of Ivy Tech Community College of Indiana will monitor group content. If a user reports inappropriate content residing on a group page the group administrator will investigate the claim and remove the group if it is in violation of the "Groups Policy".
5. The group administrator has the authority to change any parameters on the group request application, including, but not limited to, the group category, targeted roles, and misspellings in the group title or group description
6. **Groups Policy:**
 - Public groups that are of general interest to students, faculty and employees will be approved. These groups must not promote activities that are illegal or that violate the rights of others. Groups soliciting business will not be approved. Group pages must not include sexually explicit material, gambling activities, unsolicited advertising or commercial

materials. Private groups may be created only if they are associated with a sanctioned group or if the group leader has obtained permission from the Dean of Student Affairs. Content posted on group pages in no way represents the opinions of Ivy Tech Community College of Indiana.

7. Membership Policy:

1. Group members should accord themselves in a professional and respectful manner when publishing content on the group web site. Members agree not to publish content that is illegal or offensive to other group members or in any other way violates college policy and agree to share their user names and e-mail addresses with other members of this group. Members may not use group web sites for the publication or distribution of copyrighted materials or licensed software. Group leaders cannot add users to their group against their will or without their knowledge. Any violation of this policy will result in immediate revocation of group membership and possibly other appropriate disciplinary actions.

Targeted Announcements Procedures:

1. There are two types of announcements that can be sent through Campus Connect:
 - A personal announcement can be targeted to user attributes, such as campus, student, faculty or employee.
 - A college announcement is system-wide message sent to every user
2. With the proper access, Regional and Central Office administrative staff can send personal and college announcements through Campus Connect. To request access, go to Campus Connect's group portal and request to join the "Targeted Announcements" group in the Statewide – Employee category. The system administrator will grant access after the applicant has received training for sending announcements.
3. Targeted Announcements will appear on the Home tab only. They can no longer be sent through the email system.
4. The footer of each announcement must contain information about the sender, including campus, sender's name and phone number or email address.
5. Announcements regarding campus closings due to inclement weather or facility problems should be send statewide as college announcements so that students and faculty attending or teaching courses at multiple campuses will receive the announcement.

Data Privacy Policy

Jan Sheets will write a statement about data privacy based on the Data Classification. The statement will say something like this: "The College has the right to...For more specific information please refer to the Student Handbook or Employee Handbook."

Acceptable Use Policy

Michele Hygema will review the Student Handbook, Faculty Handbook, and Employee Handbook to look for commonality in the acceptable use policy.

Student Computing Practices

Already written and posted on the Help Desk website.