Policy Title	Authorized Access to Information Technology Resources
Policy Holder	Senior Director, Computer Services and Project Management
Policy Approver(s)	Senior Team
Related Policies	7-1-1 Acceptable Use Policy
Related Procedures	
Appendices	
Storage Location	Website - https://www.confederationcollege.ca/policies-and-procedures
Effective Date	Oct 28, 2009
Next Review Date	January 30, 2026

Purpose

The computing and information technology resources of Confederation College support students and employees in teaching, research, administrative, and learning activity. Access to these technology resources is a privilege with specific requirements for authorized access.

Scope

This policy applies to all students, staff and stakeholders with access to Confederation College information technology resources through a login account.

Definitions

This includes an explanation of terms and abbreviations used within the policy and procedure.

Word/Term	Definition
Disabled login account	A login account that can no longer be used for access to College IT systems, but still has resources assigned to it. The account is in a suspended state.
Deleted login account	A login account that has been completely removed from College servers.

Governing Laws and Regulations

Policy Statements

1 Authorized Access

Access to Confederation College's IT resources is provided through network based user login accounts. Each student, staff, and faculty is issued a unique individual account. Attached to each account is the appropriate security and permissions necessary for the individual to access the systems and data necessary in their role at the College.

The College may also provide IT services or resources to others with whom it does business (e.g., contractors, retirees, visitors, or Board members). Such requests for account access must be made to the Computer Services Department through a department manager.

Group or shared accounts are permitted only in exceptional circumstances and are generally discouraged. Special arrangements must be made with Computer Services in such instances. Responsibility for a shared account will be assigned to an individual.

Computer Services c provide shared e-mail addresses that multiple staff can access when assigned the appropriate privileges.

Any person without an authorized College account is prohibited from using any and all College IT resources other than open access public wifi services, or specific exceptions approved and implemented by Computer Services.

2 Unauthorized Access

Unauthorized access can include, but is not limited to, the following types of actions:

- using unauthorized accounts, computer addresses or identities,
- modifying assigned network settings/accounts to gain access to IT resources or information,
- otherwise attempting to evade, disable, or hack security provisions of the College or other external systems.

Persons using any information technology facilities for which they are not authorized may be committing an offence under the Criminal Code of Canada.

3 User Responsibilities

All College IT Resource users must:

- Comply with all College policies, rules, and regulations, as well as applicable federal and provincial laws.
- Comply with all definitions of acceptable and unacceptable use, as defined in the College's Acceptable Use of Information Technology Resources policy (7-1-1).
- Use only those College computing resources that they are authorized to access and only for the purposes for which the access is granted.
- Upon request by College Security or Computer Services staff, produce a valid College Student or Staff Photo ID card, or provide some other form of appropriate identification. Failure to so may result in the individual being escorted out of computer labs or the College property.

4 Access to College Business and Learning Systems

Access to administrative College data is primarily controlled through the access rights granted within the College's administrative software – Banner. The system provides web based interfaces to data with the system: 1) self service modules (SSB and self serve dashboards), and 2) a more detailed, fully functional interfaces (Admin pages and INB) intended primarily for more intense, comprehensive use of the system.

Regardless of the interface used to access Banner, individual rights are granted within four broad areas:

- Human Resource Module
- Finance Module
- Student Module
- General Access

All users of the College administrative system will have default access rights to data specific to their relationship with the College: In particular, using self service modules:

- Employees have access to their payroll and other HR information.
- Budget holders have access to the details of their budgets and expenditures.
- Faculty have access to data for the courses they are assigned, and to students registered in the classes they teach.
- Students have access to their financial and academic information including classes in which they are enrolled.
- Everyone has access to their personal data (contact information, tax forms)

In addition to default rights, Department managers can request additional rights to Banner Admin Pages/INB. These rights are primarily grouped into security classes – sets of functional screens that are required to complete related work at the College. Ex. A security class to create a job position, create a purchase order, accept a student into a program, etc.

Individual access rights to Banner data are granted by the Banner module administrator – the College manager who has the responsibility of approving access rights to security classes within the module:

- Human Resource Module – Director of Human Resources
- Finance Module – Director of Finance
- Student Module – Registrar

Computer Services staff will implement data access changes only when authorized by the module administrator or their designate.

Access to other administrative systems is generally controlled by rights assigned in Banner, or provided explicitly in College employee onboarding checklists.

Access rights in academic learning environments are identified by the teaching assignments and class enrollments in Banner. These relationship are updated daily to the College LMS environments (ex. Blackboard).

5 Onboarding and Offboarding of Employees

When employees are hired into a position, managers must complete an onboarding process with Human Resources. This includes the identification of all system access rights and privileges necessary to do their job.

Similarly when employees retire or resign from their position, managers must notify Human Resources and complete an offboarding process. Computer Services will then be notified to remove the rights that were assigned to the employee's login account necessary to complete their job, including access to Office 365. The employee's login account will remain active for 2 years with access limited to personal information (tax forms, contact information).

The College recognizes the transient nature of some employment with the College – in particular part time staff who teach on a semester basis, but often experience expected gaps in employment (ex. summer gaps). The offboarding process will provide managers the opportunity to identify employees who are likely to be rehired. Any such identified employees will maintain access to Office 365 (and therefore College e-mail) for a period of 2 years after employment.

Managers must also inform Human Resources whenever an employee changes positions within a department or to another department. Employees are not to accumulate access privileges as they change job roles. Rather, they are only to be assigned the access rights necessary to complete their current job.

6 Student Login Account Creation and Deletion

Domestic student login accounts are created automatically from the OCAS Application process.

- Upon application to a College program students receive a base account - a login identity that enables access to Banner SSB, and an e-mail address.
- Upon confirmation to attending a program, login rights are expanded to include Office 365 licensing.
- Course access within Banner and the College LMS (Blackboard) are automatically provided once enrolments are completed in Banner.

International student accounts are similarly created, with manual intervention by the Registrar's Office required for creation of the base account.

Student login accounts are deleted 2 years after completion of the student's last course enrollment. Students will be assigned a reduced Office 365 license during the 18 month period giving them access only to their e-mail account. Also, during this period, students will continue to have access to their personal data in Banner (contact information, tax forms, grades).Student login accounts are deleted 2 years after the last time the holding student was registered in a College course.

Non-Compliance

Revision History

Version	Change	Author	Date of Change
1	Original	Paul Inkila	29-10-2009
2	Change for on/off boarding	Paul Inkila	18-4-2022