CCNY Technology Access Request – COEdu Partners

Email questions to: solutions@cu-portland.edu

User Information	
Full Name (First, MI, Last):	
Title:	
Email:	
Partner Org:	☐ CUP ☐ HotChalk
Department:	☐ Admission ☐ Registrar ☐ Student Services ☐ Financial Aid ☐ Finance ☐ HR ☐ Other: _____

Technology Information			
Access Needed:	☐ Banner	☐ BDMS (Xtender)	☐ Argos ☐ Blackboard (handled by Portland)
	☐ Email	☐ Other: _____	

Banner Access Request	
Banner Security Group: --Select Option--	**Other:**

BDMS (Xtender) Access Request	
BDMS Security Group: --Select Option--	**Other:**

Argos Access Request		
Report Name	**Add**	**Remove**
	☐	☐
	☐	☐
	☐	☐

Authorization – Requesting Supervisor		
Signed:	**Name:**	
Title: ☐ CUP ☐ HotChalk	**Date:**	

Authorization – Concordia Portland ATS	
Signed:	**Name:**
Title:	**Date:**

Security Classes	

CONCORDIA COLLEGE
NEW YORK

ITS Policy Overview

This document provides an overview of ITS Policies and Best Practices. Any questions should be directed to the ITS helpdesk.

1. Information Privacy:
    a. No information generated, communicated or stored on a corporately owned system is personally private. All information is considered property of Concordia College.
    b. Be aware of possible breaches of privacy when exporting or sending confidential data.
    c. Personally Identifiable Information (such as SSN, credit card numbers, names, birth dates, etc) must be stored in a secure location.
    d. If the data is electronic it must be stored on secure network shares, not local PC hard drives, thumb drives, CDs, etc.
    e. If the data is printed it must be stored in a secure location and shredded when discarded.

2. Acceptable Use:
    a. College owned systems, including telephones, are not to be used to spread profanity, obscenities, sexual innuendo/jokes, harassment of any kind, and are not intended for the exercise of the user's right to free speech.
    b. The primary function of the computer network is to support the academic endeavors of students, faculty and staff. Limited personal use is permissible.
    c. Access only authorized network resources. Users are prohibited from reading, modifying, deleting or copying information that is not intended for their use.
    d. College computing resources may not be used for any activity that is illegal, unethical or contrary to the educational goal of the College.
    e. Damage due to negligence or willful vandalism to College-owned systems, including telephones, may result in disciplinary action.

3. Login and Password for Users:
    a. Users must not disclose their password to anyone (including ITS staff) or write it down.
    b. Users must not share their usernames with others.
    c. Passwords must be at least 6 characters, contain at least one capital letter, one lower case letter, one non-alphabetic character, and difficult to guess.
    d. Passwords will be required to change every 6 months.
    e. Users must not leave their system unattended without logging out or otherwise securing their system.
    f. Users may not share accounts or log on for others to use.

4. Network Access for Users:
    a. Internet should be used for business activity except for limited personal use as described above.
    b. Users are prohibited from allowing others to use their username and password to access the network.
    c. Computers not owned by the College may not be used on the campus' secure administrative network.

   d. The college facilities, computers and/or LAN/Internet access are not to be used for commercial purposes or for the benefit of other organizations and entities.

5. Malicious Code and Applications for Users:
   a. Users must not install applications (programs) without assistance from a system administrator and only corporately approved applications may be installed.
   b. Users must not download software from the Internet or outside the Concordia College Network.
   c. User must report suspected virus infection to the helpdesk.

6. Electronic Messaging - Email / Instant Messaging (IM) for Users:
   a. All electronic messages are considered records of Concordia College and subject to monitoring.
   b. Users should exercise caution, using their organizational email / IM account and primarily for business activities.
   c. Users must not send or forward email of a personal nature to a large number of people (spam, chain letters, jokes, etc...). College-wide announcements must go through proper channels.
   d. Users should not open attachments that they are not expecting or are suspicious in nature. Contact the helpdesk with questions.
   e. Access to outside email accounts from within the Concordia College network is prohibited.

7. Distributed Data for Users:
   a. Users need to store all business related data to an appropriate network share drive.
   b. Users are prohibited from making resources on their workstations available as network shares to others.
   c. Users needing to share files should contact the Helpdesk for assistance.

By signing the document above, Portland's IT representative confirms the useer has been briefed and understands Concordia College - New York's use policies.