# Section 15: Technology

## 1 Technology

As an employee of Concordia University your position may require privileges which include access to the University's information resources including the network, computers, applications and the internet. Upon acceptance of your account information and signed acknowledgement of receiving this handbook you will be granted Network and Internet access in your office.

If you or anyone you allow to access your account (itself a violation) violates these terms of usage your access may be denied or withdrawn. In addition, you may be subject to disciplinary action, up to and including termination.

By accepting your account password and related information and accessing the university's information resources, you agree to adhere to these provisions. You also agree to report any network or internet misuse to Computing Services. Misuse includes interfering with the operation of Concordia's information resources and electronic data, interfering with the work of other staff, using university resources to harass individuals or using information resources to engage in illegal or unethical activities. Note that interfering with computer resources might violate Nebraska law.

Access to University information resources extends throughout the term of your employment. Specific access to particular resources is controlled based your position's needs.

Employees are required to adhere to the University's electronic writing and content guidelines and use information resources appropriately and legally. In particular, you should use electronic communication tools with civility, politeness and a concern for the welfare of others. The University will determine what materials, files, information, software, communications and other content and activity are permitted or prohibited as outlined below.

### 1.1 Banned Activity

**Banned activities include but are not limited to the following:**

- Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory, or misleading language or materials.
- Revealing personal information to anyone, such as the home address, telephone number, birth date, Social Security number, registration data or personnel information of any person.
- Making ethnic, sexual-preference or gender-related slurs or jokes, particularly in electronic communication or stored documents.
- Using University information resources to engage in illegal activities, violating the Employee Handbook or encouraging others to do so. Examples:
    - Selling or providing substances prohibited in the University's employment policy or the Employee Handbook

- Accessing, transmitting, receiving or seeking unauthorized, confidential information about students, faculty, staff, donors and constituents.
- Conducting unauthorized or non-University business.
- Viewing, transmitting, downloading or searching for obscene, pornographic or illegal materials.
- Accessing folders, files, work product, documents or other information to which you do not have authorized access or intercepting communications intended for others.
- Using the user name and password of any other user to access any University information resource for any purpose, even if that user provides the user name and password to you. Note that you should report this action to your supervisor.
- Downloading or transmitting the University's confidential information.
- Causing harm or damaging property and data of the University or any other user.
- Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the network or the internet are not marked with the copyright symbol, employees should assume all materials are protected under copyright laws – unless explicit permission to use the materials is granted.
- Using another employee's account in a manner that deceives recipients into believing someone other than you is communication or accessing the network or internet.
- Uploading a virus, other harmful software or corrupted data onto the University's information resources or vandalizing the University's information resources by disclosing or sharing passwords and/or impersonating others.
- Using software that is not properly licensed from the vendor or is not approved by the university.
- Jeopardizing the security of access, the network or other internet networks by disclosing or sharing passwords and/or impersonating others.
- Accessing or attempting to access controversial or offensive materials. Network and Internet access may expose employees to illegal, defamatory, inaccurate, or offensive materials. Employees must avoid these sites. If you know of employees who are visiting offensive or harmful sites, report that use to the Computing Services Department.
- Using University information resources to conduct unauthorized personal business, including operating a commercial vendor. Limited personal use (e.g. purchasing a book from Amazon, making an airline reservation for paid time off) is generally permitted. Always check with your supervisor to make sure your use is permitted.
- Wasting the university's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send

e-mail copies to nonessential readers. Do not send e-mail to group lists unless it is appropriate for everyone on a list to receive the e-mail. Check with your supervisor for appropriate use of university-wide e-mail tools, including university listserves.

- Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing or illegal content.

## 1.2 Confidential Information

Employees may have access to confidential information about the university, our employees, and students. Except with the approval of your supervisor, do not use e-mail to communicate confidential material. It is extremely easy for e-mails to be accidentally or inappropriately forwarded, printed or distributed. This can result in a breach of the University's privacy policy. When a matter is personal, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

## 1.3 Privacy

***TECHNOLOGY AND PRIVACY OF INFORMATION POLICY***

Computer and telecommunication technology provide a variety of means for communicating and transferring information. These include, but are not limited to, electronic mail, voice mail, telephone communication, cellular communication, and video communication. Technological developments may incorporate other forms in the future.

All faculty, staff members, and students are advised that:

1. The technology to which you have access, the information stored in it, and the information transferred through it are the property of Concordia. These facilities and resources are for use in carrying out your duties as an employee or as arranged by Concordia with students. Appropriate personal use is also permitted within these same limitations. Commercial use is prohibited.

2. During the course of normal maintenance operations, during checks to insure security, or at the request of the president, authorized personnel may monitor the use of these facilities and resources, and they may examine information found there. You have no reasonable right of privacy while using these Concordia-owned systems. You have no reasonable expectation of privacy while using these or any other Concordia-owned systems or property. The University reserves the right to monitor the work, work areas and work product of its employees.

3. Any activities or information deemed inappropriate by Concordia or which may be unlawful will be reported to the proper authorities for further action. Inappropriate activities include, but are not limited to, viewing or transmitting obscene materials, harassment of any sort, and interfering with the use of these facilities by others. Concordia will cooperate fully with law enforcement agencies in their investigation of unlawful events.

## 1.4 Noncompliance

Your use of the University's information resources is a privilege, not a right. Violate these guidelines and, at minimum, your access to these information resources will be terminated, perhaps for the duration of your tenure with the university. Breaches include violating provisions described in this Handbook and by failing to report violations of other users. Permitting another person to use your account or password to access the University's information resources, including, but not limited to someone whose access has been denied or terminated, is a violation of these guidelines. Should another user violate these guidelines while using your account, you will be held responsible and both of you will be subject to disciplinary action. Criminal violations may lead to criminal or civil prosecution.

## 1.5 Electronic Mail

The university provides employees with electronic communications tools, including an email system. These guidelines govern employees' use of the e-mail system, apply to use of the University's email systems whether such access is from on-campus or from off-campus locations, including, but not limited to the employees' homes, airports, and hotels. The university's email rules and guidelines apply to full –time employees, part-time employees, independent contractors, interns, consultants and other third parties. Any employee who violates these guidelines is subject to disciplinary action, up to and including termination.

The university e-mail system exists primarily for business purposes. Employees may use the university's e-mail system for personal use only in accordance with this policy. An employee should not use personal email software (Hotmail, etc) for business or personal communications at the office, without prior approval of your supervisor.

Employees may use email to communicate with spouse, children and other family members. Personal use of email should normally be limited to lunch breaks and work breaks and, in any case, must not interfere with worker productivity during business hours. Employees should not use email during otherwise productive business hours. Employees are prohibited from using email to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit fund for other personal causes.

E-mail messages created, transmitted and stored on university computer systems are the property of the university. The university reserves the right to monitor all e-mail transmitted via the university computers system. Employees have no reasonable expectation of privacy when it comes to business and personal use of the university's e-mail system.

At any time and without notice, any and all usage of email and any and all files, information, software and other content created, sent, received, downloaded, uploaded, accessed or stored in connection with employee usage, may be monitored, inspected, copied, reviewed and stored.

Employees are prohibited from using email to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

Unless authorized to do so, employees are prohibited from using email to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information abut the university, employees, students, vendors and other business associates. Confidential information includes, but is not limited to employee lists, credit card numbers, Social Security numbers, employee performance reviews, salary details, student lists, passwords, and information that could be detrimental to the university and employees, students, alumni, donors and others in the Concordia community were it to be inappropriately distributed.

Email messages are considered to be written business records and are subject to the university's written and consistently applied rules and policies for retaining and deleting business records. E-mail records are also written documents that are discoverable as evidence for legal purposes.

## 1.6 Software

Concordia University requires that all software used by Concordia-owned computer systems be properly and legally licensed for use at the university. All Concordia University employees, in the performance of their duties, will refrain from aiding others in using software that is not properly licensed. Should any Concordia employee use inappropriately licensed software on a university-owed computer, the responsibility for the consequences of such activity shall remain the sole fiscal and legal responsibility of the offender.

Computing Services is responsible for the administration of all software products and the deployment of such software. Please contact Computing Services for questions regarding acquiring and using software legally and appropriately.

## 1.7 Data Security

Data is considered a primary asset for Concordia University. As such, security of data is necessary in today's environment because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems creates a unique vulnerability for Concordia University.

Security and privacy both focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of confidential data; violate student and employee privacy; or reduce our credibility and reputation with other entities.

Our objective here CUNE is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure or destruction. This policy applies to all of our data assets that exist in any of our processing environments (collectively all applications, systems, and networks that we own or operate or that are operated by our agents).

Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need-to-know basis to specifically identified, authenticated, and authorized entities.

A data security breach would have severe consequences to CUNE and its ability to provide services. Intentional misuse resulting in a breach of any part will result in

disciplinary action up to and including termination and criminal investigation where warranted and subject to civil criminal penalties.

It is the responsibility of all employees to immediately report any data breach, intentional or accidental, to both your supervisor and to Computing Services (643-7321).

While the data security is the responsibility of every employee, it is overseen by Computing Services and the Critical Incident Management Team.

## 1.8 Destruction of Sensitive Materials

Hackers and industrial spies have long used “dumpster diving” as a method for gathering sensitive information which has taken on new meaning in the electronic information age. Sensitive materials must be thoroughly sanitized before being discarded whether in print or electronic form.

Papers with sensitive and personally identifiable information should be placed into the locked shred bins located in various buildings on campus. CUNE has hired a shredding company to come to campus and shred these types of documents. Check with your supervisor to determine the location of the shred bin for your work area.

For disposal of other types of electronic media – CD-ROMS, external storage devices, or magnetic media, please consult Computing Services for assistance.

## 1.9 Backup Your Data

In order to ensure that any University documents are properly backed up, they must be stored on a University file server. Check with your supervisor and Computing Services for proper access procedures. Specifically, any files stored locally on your computer rather than on a University file server may be lost in the event of a hardware failure.

## 1.10 Systematic Removal of Access

Unauthorized access to University information resources can cause serious damage to the organization. Disgruntled employees can use lingering accesses to enter systems or office space. Hackers can use inactive accounts to enter systems unnoticed. Potential damage includes theft of funds, equipment or intellectual property, disclosure of confidential information, and/or damage to property or personnel.

When an employee leaves their accesses must be immediately revoked. Human Resources initiates systematic removal of accesses with Computing Services. When a consultant leaves, their supervisor must ensure accesses are removed. Employees must only have the accesses their position requires. When roles change, supervisors must rescind unneeded accesses.

Each department has unique accesses that must also be addressed. When an employee leaves, the employee or their supervisor will contact financial institutions, vendors, and any other external organizations where the individual is listed as a point of contact in order to update external contact lists and change authorization passwords. Removal of access should be documented and routine.

## 1.11 Laptops

The loss of a laptop can cause irreparable harm to the organization. Laptops must be secured and used responsibly to prevent compromise of sensitive information or unauthorized network access.

Computing Services has taken measures to address the threats laptop users face. Your active involvement is critical to complete the equation.

- Do not leave a laptop unattended at any time.
- Laptops are equipped with firewall software to defend against hacking attempts on public networks and the Internet.
- Electrical surges: You may wish to protect your laptop from electrical spikes by plugging its power into a working surge protector when possible.
- The loss of a laptop is a serious security incident. In the event a laptop is lost or stolen, or you believe it may have been used or compromised by a third party, immediately contact Computing Services.

## 1.12 Unauthorized Disclosure

Unauthorized disclosure of sensitive information represents a serious threat to the organization. Unintentional disclosure can occur over the many distribution methods available today: Websites, databases, application software, files, printouts, e-mail, phone, and voicemail. Each must be carefully controlled. One common mistake is forwarding internal e-mail to external parties with sensitive information attached in a file or buried at the bottom of a long string of messages. Internal e-mail addresses may be inappropriately shared in this manner as well.

Do not disclose sensitive or personally identifiable information to consultants or coworkers, unless they have a business related need-to-know that has been approved by your supervisor. Key questions for both you and your supervisor are “What are you using the information for?” and “Who will you share it with?”

There may be penalties for disclosing sensitive information to unauthorized persons.

Section 15: Technology

I have received a copy of Section 15 – “Technology” from the Concordia University Employee Handbook. I have been informed that the terms, rules and conditions in this section apply to me as a contracted employee for Concordia University. I understand all of the rules, terms and conditions and agree to abide by them, realizing that failure to do so may resulting in termination of service as a contracted employee.

_____

Printed Name

_____ _____

Signature Date