IT01: APPENDIX 2

ALGONQUIN COLLEGE IT RESOURCE USER AGREEMENT FOR EMPLOYEES AND CONTRACTORS

Managers must keep copies of these signed agreements. Digitized copies may be kept within Workday.

On being issued an Algonquin College account User ID and email account, I agree that:

GENERAL

1. I will not apply for a User ID under pretenses.
2. I am the sole person authorized to use my User ID.
3. I am solely responsible for all actions taken using my User ID.
4. I will not allow others to use my User ID.
5. I will not use the access I am provided to peruse or obtain information for purposes that are unrelated to my job function ("snooping").
6. I will use strong passwords for my College User ID and applications that meet the College's Information Security Policy (IT01) and related Directive password creation requirements. Password creation and update must conform to the following rules
    a. Minimum 8 characters (12 for privileged accounts)
    b. Must contain uppercase letter
    c. Must contain lowercase letter
    d. Must contain number or special character
    e. Must not contain portion of first or last name
    f. Can only reset password once per 24-hour cycle
    g. Password must be unique, and the past 6 passwords must not be used
    h. Password must be changed every 180 days
7. I will not use College IT resources for personal gain, commercial or fraudulent purposes.
8. I will not examine, copy, modify or delete information belonging to other users without prior consent.
9. I will not make any unauthorized, deliberate action that damages or disrupts an IT resource, alters its normal performance, or causes it to malfunction.
10. I will report any suspected or actual security violation, security incident, privacy breach or criminal act to the Manager, Information Security and Privacy or by sending an e-mail to infosec@algonquincollege.com.
11. I further acknowledge that the information transmitted or stored, and the activities undertaken on College technology systems and equipment may be subject to monitoring. The College will not use monitoring or examination of the information described in this paragraph for the purpose of routine monitoring of employee productivity or performance, but may use the information in the course of investigations in the workplace.

COMPUTING AND NETWORKING SECURITY

1. I will protect my College provided computer at all times from loss and theft.
2. I will use a College provided computer at all times to conduct College business, including while working at the office, at home and while travelling on College business, if I am a full-time employee.
3. I will use a College provided computer at all times to conduct College business, including while working at the office, at home and while travelling on College business, if I am a part-time employee or contractor and will be handling a significant amount of sensitive learner, employee or other

information.

4. If using a personal computing device (e.g., desktop, laptop, tablet) to access College IT resources, I will ensure that it has whole disk encryption turned on, its operating system and anti-malware software is kept current, and it is not connected to any other network at the same time while connected to the College network.
5. If using a personal computing device (e.g., desktop, laptop, tablet, home computer), I will ensure at the end of my employment or contract that all information is returned to the College and any copies or remnants are securely destroyed.
6. I will use a password enabled screen saver set to a period of inactivity (15 minutes or less).
7. I will not use an unencrypted USB drive or unencrypted external hard drive to store sensitive College information.
8. I will not attempt to access IT resources that I am unauthorized to use or attempt to secure a higher level of user privilege within applications, other than what I have been authorized.
9. I understand that Microsoft OneDrive is the only official information cloud storage system for College use. I will not use third-party 'cloud' information storage services (e.g., personal OneDrive account, Dropbox, Google Drive) for the storage of College information.

EMAIL

1. I am solely responsible for all electronic mail originating from my User ID, even though I may share my e-mail account with an assistant or authorized user using the "delegated access" function.
2. I will only create messages that are necessary for the conduct of College business using my College provided e-mail account, although I may send and receive limited and reasonable non-College personal messages which are incidental to and do not interfere with the primary business use of the College's electronic messaging systems. I understand that such messages must still comply with this policy in all respects.
3. I will communicate with learners using their College provided email accounts. I may use learners' personal email accounts, either before they receive their College provided email account, or for backup or emergency purposes; however, I will not communicate sensitive personal information using the learner's personal email accounts unless email encryption is used.
4. I will not forge or attempt to forge electronic messages.
5. I will not send unwelcome, unwanted, offensive, intimidating, derogatory, hostile, threatening, pornographic or otherwise inappropriate messages to another user.
6. I will not send unsolicited 'for-profit' messages or chain letters.
7. I will not send unauthorized network broadcast messages.
8. I will not send solicitation emails to external recipients that do not have a formal business relationship with the College. I understand that this 'spam' could violate the Canadian Anti-Spam Legislation (CASL) and put the College at reputational and legislative compliance risk.
9. I will be careful not to misdirect emails to unintended recipients, particularly emails containing sensitive information. I understand that this could lead to a serious privacy breach.
10. I will not send unencrypted Word or Excel email attachments containing significant sensitive learner or employee information.
11. I will be careful not to click on suspicious e-mails, including phishes, but will instead use my "Report Phishing" email ribbon icon, when possible, to report and securely delete the suspicious emails.
12. I will include the following notice at the bottom of all my College emails: *"This email is intended solely for the addressee(s) and is Confidential. If you received this in error, any disclosure, copying, or distribution is prohibited. Please reply and inform the sender and delete all copies. Thank you."*

MOBILE PHONES

1. I understand that Apple iPhone is the College's preferred mobile phone technology and that Android or other mobile phones can only be purchased, on an exception basis, with the review and permission of the Manager, Information Security and Privacy.
2. I will always use a minimum of a six-digit PIN to protect access to my mobile phone, including for

College-owned mobile phones as well as personal mobile phones used to access College IT resources. I will not share my six-digit PIN with anyone.

3. I will not use a 'jail-broken' or 'rooted' (weakened operating system) mobile phone to connect to the College network.
4. When using a personal mobile phone to access College IT resources, I will ensure that its operating system is kept current, and it has anti-malware software that is kept current.
5. I understand that Mobile phone text messaging must only be used for limited operations requirements and should not be used to replace corporate email messaging, to ensure that the College maintains official records in support of information access requests.
6. I will only create text messages that are necessary for the conduct of College business using my College provided mobile phone, although I may send and receive limited and reasonable non-College personal text messages which are incidental to and do not interfere with the primary business use of the College's electronic messaging systems. I understand that such messages must still comply with this policy in all respects.

I have read, understood and agreed to use my account(s) per this agreement.

I accept full work-related, professional and legal responsibility for all of my actions while using the College's IT resources.

_____

Employee/Contractor Name (Print)

_____

Employee/Contractor Signature

_____

Date (DD/MM/YYYY)

(Provide one signed copy to the User and keep one copy in Manager's office)