ALGONQUIN COLLEGE | Cyber Security Unit

Protecting Learner and Employee Information While Working Remotely off Campus

Security and Privacy Guidelines

Version 1.1

Overview

All employees need to understand the cyber risks associated with working from home as well as be aware of ITS's recommendations for computer use, where to store College information, the security practices for email and mobile phones, how to report security and data breaches, and more. The following guide is a must-read for all employees working off-campus.

Algonquin College's Information Sensitivity and Security Policy (IT05) states:

1. *Employees, students, contractors, vendors and volunteers of the College will take reasonable steps to protect the privacy, integrity, and availability of College information they access.*

What Cyber Risks Have Changed as a Result of COVID-19?

Cyber criminals are taking full advantage of the COVID-19 situation. The main cyber risk is increased email phishing and texting "smishing" attacks. Employees should carefully inspect emails and texts before acting on them, particularly if they come from external senders, the COVID-19 situation is mentioned, they contain an urgent call to act, or the content seems out of place.

As well, employees should only surf to those websites are that are generally trusted. Cyber criminals will try to infect less trusted and less secure websites with malware, particularly websites that provide COVID-19 information.

What Computer Should I Use?

All full-time employees must use a College-owned laptop computer unless they were provided a desktop computer instead. If you have not been provided with a College-owned computer, please contact the ITS Service Desk to obtain a laptop. These have been appropriately configured for security, including malware protection and whole disk encryption.

If you are a full-time employee that was issued a desktop computer, a part-time employee or a contractor and have not been provided with a College-owned laptop, you will likely need to use your own personal computer. Please ensure:

1. Quality anti-malware software is installed, frequently updated, and comprehensive scans are run on a regular, weekly basis. This is equally important for Windows computers as it is for Apple Macintosh computers. This protection should include firewall, file, email and web surfing protection. Quality solutions include Windows Bitdefender (for Windows computers only), AVG, AVAST, Bitdefender, Norton and TotalAV.

2. Whole disk encryption is enabled if possible (e.g. Windows Bitlocker or Macintosh File Vault)

3. A password enabled screensaver is used.

What General Security Practices Should I Follow?

All employees should:

1. Use minimum 12-character passwords, including one upper case, one lower case, one number and one special character for all of your accounts.

2. Physically protect your computers from loss and theft at all times. Never store a computer in a vehicle unintended, or if you must for a short period, place it where it can not be viewed, such as in a trunk.

3. Undertake your work in an area of the home where 'shoulder surfing' and overhearing by others is prevented.

4. Lock your computer screen when not at your computer.

5. If you print a sensitive document, make sure to protect it and shred it when no longer required.

6. Secure your home Wi-Fi. Change the default administrator password to a strong one, create strong connection passwords, and enable WPA2 encryption.

7. Log on to the College's VPN service at least once per week, so that your College-owned computer can receive important security updates.

Where Should I Store My College Information?

Employees should store College information in Microsoft OneDrive, the College's official cloud-based information storage solution. It is secure, uses your College credentials to access it, and adequately backs up your information. You should never use other non-approved solutions such as Dropbox, Box or Google Docs as these have many security concerns.

Employees may also use other College licensed Microsoft storage solutions such as Teams and SharePoint Online.

Word and Excel files, if they contain learner or employee personal information, should be encrypted, and the password shared with others 'out of band' (e.g. over the phone, or in a separate email).

Do not store sensitive documents on regular unencrypted USB drives – only use encrypting USB drives.

Employees should not use third-party applications or other technology solutions to collect and store College learner and employee information unless the College has a contract in place with the solution provider. Data sharing with these entities when the College does not have a contractual relationship represents an unauthorized disclosure of personal information for which the College could be liable under privacy legislation.

What Email Security Practices Should I Follow?

Be very careful about suspicious emails. Continue to use your “Report Phishing” email tool to report phishing if using an Outlook client. If you are not certain about the email’s origin, use a phone to call the originator using a known phone number, not a phone number provided in the email.

Employees, whether full time or part-time, must always use College email accounts to conduct College business. The College’s Microsoft Outlook contains phishing attack link protection called “Safelinks,” whereas personal email accounts do not.

Employees must use their official algonquincollege.com email accounts to send email communications to learners at their algonquinlive.com email accounts, whenever possible.

Limit the amount of sensitive learner and employee information that you send in email.

Never send unencrypted Word or Excel documents containing significant learner or employee personal information as attachments to an email. Always use encrypted documents and share the password with others ‘out of band’ (e.g. over the phone, or in a separate email).

Be very careful to double-check the recipient(s) email addresses before sending in order to avoid a misdirected email data breach situation.

What Mobile Phone Security Practices Should I Follow?

The College provides College-owned mobile phones to approximately 350 employees, particularly those that handle a significant amount of sensitive learner or employee information such as managers, executive assistants, Human Resources employees and others. Soon, College owned phones will be provisioned with Symantec anti-malware software.

If you use your own mobile phone to access College email and data make sure that you install quality anti-malware software, ensure that it is frequently updated and comprehensive scans are run on a regular basis. Privacy calling can be turned on in the phone’s settings. Another option is to precede the number being called with #31#

All employees should:

1. Use a 6-digit PIN or biometrics to protect access.

2. Limit downloads of applications that are trusted, after reading the Terms of Use to ensure that you are not providing permission for an App to access and copy data.

3. Be careful not to click on links or open attachments in suspicious texts or in personal email.

Reporting Security Incidents and Data Breaches

It is important that you immediately report suspected and actual security incidents, including loss and theft of equipment, and data breaches should they occur. Often the impact can be reduced if dealt with immediately.

Please report these to the ITS Cyber Security Unit here: csu@algonquincollege.com

Where Can I Obtain Additional Information?

Here are some excellent short videos:

Working remotely

Creating a cyber secure home

Email and Phishing

Social engineering

For further assistance, please contact the ITS Service Desk at 5555 or 5555@algonquincollege.com