1. Purpose
The purpose of this policy is to provide students with guidance on acceptable and unacceptable use of the College’s Information Technology (IT) resources. In addition, this policy supports effective organizational security and protects users and IT resources from but not limited to cyber criminals, bullying, misuse of accounts and assets, and the spread of malicious software.

2. Application and Scope
This policy applies to all students that use any component of the College’s IT resources regardless of the physical location or device used. This policy excludes student workers while performing job duties. Outside of student working hours, student workers are governed by the ‘Acceptable Employee Use of IT Resources Policy.’

3. Definitions

“Authenticate” refers to the process of logging onto an IT resource by validating a user’s identity. This is typically completed by providing a username and then validating that username by providing something you know such as a password, something you have such as a card, or by providing something you are – such as a biometric piece of information (fingerprint, retina scan, palm, etc.).

“IT Infrastructure” refers to software, hardware, devices, networks, server systems, data storage, data centres, related equipment, and cloud-based technologies.

“IT resources” refers to any IT Infrastructure component that can be interacted with and used by individuals such as a computer, application, mobile phone, data, etc.

“Sensitive Information” includes information that should not be shared and may include restricted, confidential, or personally identifiable information or documents.

“User(s)” includes any student that uses or operates an IT resource.

4. Principles
This policy is based on five key principles:

   A. Ethics, Values and Fairness
Exercise common decency, good judgement, and respect for the College community members and property.

B. Security
Preserve the integrity and availability of systems and services and ensuring that actions taken by College community members do not negatively affect College IT resources.

C. Privacy
Protect and safeguard College IT infrastructure and information.

D. Compliance
Use of IT resources adheres to all legal, regulatory and College policy requirements.

E. Productivity
Access to IT resources is uninterrupted and accessible when needed.

5. Accountability and Compliance

5.1 Accountability Framework
This policy has been approved by the Senior Leadership Team.

5.2 Compliance
The Chief Information Officer, in cooperation with other departments, will monitor and ensure compliance with this policy.

6. Roles and Responsibilities

6.1 Chief Information Officer
The Chief Information Officer is responsible for the security of all IT resources.

6.2 Employees

- Communicate relevant IT policies and procedures to students;
- Report suspected IT security incidents (See Appendix A); and
- Be compliant with the ‘Acceptable Employee Use of IT Resources Policy.’

6.3 Students

- Be familiar with College IT policies and procedures.
- Use IT resources in a safe and respectful manner that does not negatively affect the student experience.
- Protect the confidentiality, integrity, and availability of IT resources.

7. Rules

7.1 Authorized Use
All students using Mohawk College IT resources must use those resources to carry out the functions for which they were provided, specifically:
• Access to IT resources shall only be provided to active students or applicants whether they be full-time, part-time, continuing education, distance education, apprenticeship, or other.
• Access to and use of IT resources is limited to those which the student is authorized to use.
• Students must authenticate into systems using their own College provided account and should not use any other user account other than their own when accessing IT resources.

7.2 Personal Use of IT Resources

7.2.1 Students may use IT resources for limited personal use. However, browsing must be limited to well-known and reputable websites and not threaten the security or availability of IT resources. Access to IT resources must be preferentially given to those requiring use for academic purposes.

7.2.2 Personal files stored on IT resources will not be accessible or returned after the student leaves the College, whether that be after graduation, or for other reasons. Some exceptions will apply based on specific situations.

7.3 Prohibited Use
All students using Mohawk College IT resources are strictly prohibited from:

• Using IT resources for any commercial activity, or, for conducting any personal business in which they would receive personal or financial gain unless they have received permission from the College in writing.
• Using IT resources in a way that interferes with the student experience (including student well-being and success), College operations or business, or, creates any monetary cost to the College.
• Exporting software from the College for resale or distribution.
• Destroying, vandalizing or purposefully damaging or altering College IT resources and infrastructure.
• Downloading video, audio, software or any other resource that is protected by copyright law. Students acknowledge that the College will notify copyright abusers in the event the College is served a copyright claim due to a copyright infringement by their account.
• Accessing or creating illegal, disruptive, abusive, intimidating, harassing, pornographic, or obscene content.

7.4 Security

7.4.1 Users of IT resources must not knowingly place the security of information or systems at risk. At all times, Users must:

• Contact the IT Service Desk immediately in the event of an IT security incident, see Appendix A for procedure.
• Keep secret authentication information such as passwords, pin codes, or any other authentication information secure and at no time share authentication information with any individual.
• Do not leave saved work on College provided computers.
• Never install untrusted software or applications on IT infrastructure or resources. If absolutely required, always make sure that the software is obtained directly from the software vendor’s website, and ensure that the software vendor is a known good vendor.
• Ensure that personally owned devices that connect on campus are protected with antivirus software, a personal firewall, and regularly install security updates and patches to operating systems, applications, and web browsers.

7.4.2 No individual shall knowingly breach, compromise, endanger or threaten the College’s IT resources, attempt to do so, or allow others to do so. This includes probing, scanning, assessing or penetrating College IT resources. Users must report any misuse of IT resources to the IT Service Desk, or to the Chief Information Officer. Failure to report misuse may result in the assumption that the User who witnessed the misuse was party to the act.

7.4.3 Mohawk College reserves the right and responsibility to protect the College and community members from inappropriate use of IT infrastructure and resources by taking actions, including but not limited to:
• Monitoring systems, networks, services, accounts, and web activity.
• Providing access to only current active students.
  o Termination of student relationship will disable access to all College IT resources and all IT assets must be returned.
• Denying a user the right to access IT resources at any time the College deems necessary.

7.5 Compliance
Use of the College’s IT resources is subject to, and must comply with, all applicable laws and College policies and procedures, including this policy. Non-compliance with applicable laws and regulations may result in civil liability or criminal prosecution. The College reserves the right to restrict or deny access to its IT resources, to monitor your use of those resources and to take actions it deems necessary or appropriate to protect College IT resources. By using the College’s IT resources, Users are confirming agreement with this policy.

In addition to the above, Users of IT resources must also comply with:
• Applicable College policies, procedures and standards;
• Copyright Laws including, but not limited to, the sharing of pirated software, audio, and video;
• Licensing agreements; and
• Any other agreements between the College and an external service provider.

7.6 Noncompliance
Noncompliance with this policy may result in disciplinary action in accordance with Appendix C of the Student Behaviour Policy. Additionally, noncompliance with this policy may also result in the recovery of costs due to damages or fees and/or criminal or civil action.

8. Policy Revision Date

8.1 Revision Date
September 2020

8.2 Responsibility
The Chief Information Officer will review this policy every three years or earlier where required.

9. Attachments
Appendix A - Reporting an IT Security Incident

10. Specific Links
SS-3200-3206 Student Behaviour Policy
SS-3205-2017 Student Rights and Responsibilities Policy Framework
SS-3206-2016 Student Success Policy Framework
GC-4301-1982 Student Human Rights Policy
CS-1500-2013 Web Posting and Electronic Notifications Policy
GC-4100-2013 Intellectual Property Policy
GC-4101-2013 Copyright Policy
GC-4200-2013 Social Media Policy
Privacy and Legal Statements
Copyright Act
Appendix A
Reporting an IT Security Incident

What is an IT Security Incident?
An IT Security Incident is an incident that may affect the confidentiality, integrity or availability of the College’s IT infrastructure through unauthorized access or accidental disclosure, including:

- The presence of any form of malicious software (malware, viruses, worms, etc.).
- The presence of any abnormal software that was not previous present on a computer or server.
- Suspicion that your user account has been compromised.
- Web browsers re-directing automatically or producing popup messages or advertisements unexpectedly.
- File types, formats, or naming conventions changing unexpectedly or files not opening as expected.
- Slow computer performance, applications hanging, or any unexpected behaviour.
- Notifications that anti-virus or firewalls are not running or are disabled.
- Lost or stolen devices including but not limited to laptops, mobile phones, desktop computers, portable storage devices, switches, etc.

Reporting an IT Security Incident

1. Disconnect the network cable from the computer.
2. Do not power off the computer.
3. **Contact the Mohawk College IT Service Desk immediately** by phone if you believe you are experiencing an IT Security incident regardless of your location.
   - Phone: 905 575 1212 x2199
   - E-mail: helpdesk@mohawkcollege.ca

4. Make notes about the IT incident to make sure that you can provide clear and accurate information to IT staff.
   - When making notes, consider the following:
     i. What happened?
        1. What websites have I visited recently?
        2. Have I received any suspicious e-mails that were actioned recently?
     ii. When did it happen? (specifically at what time)
     iii. Where did it happen (Physical Location and Network Location (ex: Wireless))?
     iv. Who was involved?
     v. Could there be sensitive, personal or confidential information at risk?