CÉGEP Heritage COLLEGE

23

CÉGEP HERITAGE COLLEGE
POLICY #23

CONCERNING
DIGITAL NETWORKS

COMING INTO FORCE: September 28, 1999

REVISED: June 19, 2024
September 17, 2025

ADMINISTRATOR: Director of Information Systems and Technology

CÉGEP HERITAGE COLLEGE POLICY #23
CONCERNING DIGITAL NETWORKS

Preamble

CÉGEP Heritage College (hereinafter referred to as the "College") provides access to its digital networks as a vital resource for students and employees. These networks are designed to support the fulfillment of the College's mission and educational goals. They foster innovative communication and responsible information sharing within the College community, enhance public education, and promote sustainable development values. As a core component of institutional information infrastructure, the Internet connects the College to a global knowledge ecosystem. This facilitates research, outreach, public engagement, and reinforces the College's visibility and reputation.

Recognizing that the use of digital networks introduces both opportunity and risk, the College adopts a governance-driven approach based on accountability, transparency, and responsible innovation. The present Policy aligns with the following legal, regulatory, and policy frameworks:

- *Act respecting the governance and management of the information resources of public bodies and government enterprises* (CQLR, c. G-1.03),
- *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, c. A-2.1) ("Law 25"), and
- *Archives Act (CQLR, c A-21.1).*

By embedding these obligations into its digital governance framework, the College ensures that its networks and AI-enabled systems are used in ways that protect individual rights, maintain institutional integrity, promote transparency and trust, and comply with all applicable legal and ethical standards. The present Policy supports a responsible digital environment that advances the College's educational and operational objectives.

ARTICLE 1
Purpose

The present Policy aims to define clear expectations for acceptable use of the College's digital networks. It outlines permitted activities and specifies prohibited behaviors to prevent misuse that could jeopardize College operations or lead to legal liabilities.

ARTICLE 2
General Provisions

Digital networks at the College are available to students, staff, and other authorized individuals for activities directly related to academic and administrative functions. Personal use is permitted under conditions that it occurs during personal time, does not generate additional costs, nor involves financial gain. All network activities must comply with the present Policy and violations will be addressed promptly and fairly.

ARTICLE 3
Application

The present Policy applies to all members of the College community who have access to digital network resources, including staff, students, contractors, and individuals who have entered into a working or service relationship with the College. This includes access to systems and services that leverage or interact with Artificial Intelligence (AI), such as automated decision-making tools, machine learning models, generative AI platforms, and AI-enabled academic or administrative systems.

The present Policy also extends to remote access situations, including telework and other off-campus activities, where College digital resources or AI-powered services are used. All users are expected to interact with these technologies in accordance with institutional values, applicable legislation, and responsible use standards defined by this Policy and relevant provincial guidelines.

ARTICLE 4
Authorized and Prohibited Uses of Digital Networks

4.1 Authorized Uses

This section delineates the authorized activities on the College's digital networks, designed to support the institution's operational and educational objectives. All members of the College community are expected to utilize digital resources responsibly and ethically, within the bounds of institutional policies and legal standards. The following activities are illustrative of authorized uses, provided they adhere to the guidelines stipulated:

4.1.1 Professional and Academic Use

- **Work and Study Functions:** Using digital resources to fulfill assigned professional, academic, or research responsibilities consistent with the College's strategic objectives.
- **Collaboration and Communication:** Sharing information with colleagues, students, public partners, and professional contacts, provided such exchanges do not compromise confidentiality, privacy, or institutional security.
- **Professional Development:** Accessing approved online courses, webinars, or training activities that support skill development related to one's role.

4.1.2 Responsible Resource Use

- **Approved Software and Tools**: Acquiring or using licensed or institutionally vetted software, cloud platforms, or applications that enhance teaching, learning, or operational efficiency.
- **Reasonable Personal Use**: Limited personal use of digital resources during personal time is permitted if it does not interfere with work, consume excessive resources, or contravene College policy.

4.2 Prohibited Activities

Any use of the College's digital networks that undermines cybersecurity, violates applicable laws, or conflicts with College policies is prohibited. Engaging in any of the prohibited activities listed below may result in disciplinary action up to and including termination of access, dismissal from the College, legal action, and criminal charges where applicable. Prohibited activities include, but are not limited to:

4.2.1 Security and Confidentiality

- **Unsecured Transmission**: The transmission of confidential information, including personally identifiable information (PII), over unsecured networks is strictly prohibited unless it is encrypted in accordance with the College's security standards. Unsecured networks refer to networks external to the College. When accessing College resources or transmitting sensitive data from outside the premises, users are required to use the College-approved Virtual Private Network (VPN) to ensure secure communications.
- **Unauthorized Access**: Attempting to access, use, or share data, systems, or accounts without explicit authorization.
- **Security Breach**: Attempting to bypass, disable, or compromise security controls such as firewalls, intrusion detection, or encryption.

4.2.2 Network Integrity and Usage

- **Resource Abuse**: Activities that disrupt or degrade network performance, such as mass mailings, unauthorized cloud mining, or excessive streaming.
- **Unauthorized Software**: Installing, downloading, or operating unapproved software, applications, or devices that could compromise system integrity.

- **Malware Distribution**: Uploading, hosting, or spreading viruses, ransomware, spyware, or other malicious code.

4.2.3 Content and Standards

- **Illegal or Inappropriate Material**: Creating, accessing, storing, or distributing obscene, pornographic, exploitative, or violent material.
- **Abusive or Discriminatory Communication**: Sending messages or content that are abusive, sexist, racist, threatening or harassing in nature, defamatory, or otherwise discriminatory or offensive to any individual or group is forbidden.

4.2.4 Representation and Expression

- **Misrepresentation**: Representing personal viewpoints such as endorsements or statements of the College without explicit authorization by the Director General undermines the integrity of the College and is prohibited.
- **Political Activity and Public Criticism**: Using College resources to engage in political activities or to publicly criticize government policies or actions in a manner that implies College endorsement is prohibited unless such activities are directly related to one's academic or professional responsibilities and are approved by the Director General.

4.2.5 Unlawful Activities

- **Cybercrime**: Engaging in hacking, unauthorized access, destruction, or alteration of data, spreading malicious software, or any activity designed to compromise the security of computer systems and networks.
- **Intellectual Property Violations**: Infringing upon the copyrights, trademarks, or patents of another without authorization.
- **Fraud and Illegal Activities**: Using the network to commit fraud, extortion, bribery, illegal gambling, or other criminal acts.

ARTICLE 5
Monitoring

5.1 Purpose of Monitoring

The College is responsible for ensuring compliance with the present Policy and other institutional policies and legal requirements. Because of this obligation, it is essential to acknowledge that monitoring of digital network activities is a necessary component of our governance and security strategies.

5.2 What Is Monitored?

- **Network Traffic and Data Flow**: This includes monitoring the volume of data transmitted, session durations, and the types of protocols used. Monitoring traffic helps in managing network bandwidth and identifying unusual patterns that could indicate security threats or network abuse.
- **Access Logs**: We keep detailed logs of system and network access. These logs include User identifications, timestamps, the devices used, and the nature of the data accessed. This information is crucial for auditing and could be used in investigating policy violations or breaches.
- **Email and Communication Systems**: All inbound and outbound communications are subject to monitoring for compliance with legal standards and institutional policies. This includes checks for malicious content, spam, and unauthorized information sharing.
- **File and Resource Access**: Monitoring who accesses what resources is vital for ensuring that sensitive or confidential information is not being improperly accessed or shared. This includes real-time analysis of access patterns and permission checks.

- **User Activities and Behavior**: Real-time monitoring of actions on the network, such as file downloads/uploads, website access, and software usage, to ensure compliance with our acceptable use policies and to prevent the distribution of prohibited content.
- **Security Systems and Controls**: Regular checks on the effectiveness of our cybersecurity measures, including firewalls, intrusion detection systems, and anti-malware tools, to ensure they are functioning correctly and protecting our network as expected.

5.3 Privacy Considerations

While monitoring is essential for operational and security purposes, the College is committed to respecting the privacy of all network Users. Monitoring activities comply with applicable privacy laws and regulations, including the Charter of Rights and Freedoms and Law 25. Information obtained through network monitoring is used strictly for compliance, security, and operational efficiency purposes and is handled confidentially.

5.4 Reporting and Incident Response

Any findings from monitoring activities that suggest policy violations or security incidents are documented and handled according to our incident response procedures. This includes immediate notification of relevant authorities within the College and, if necessary, external law enforcement agencies.

ARTICLE 6
Access to Information

The College ensures that all network activity logs are maintained with strict adherence to privacy and security protocols. These logs detail websites visited, email addresses contacted, and the identity of the computers within the Service or department that initiated these contacts. Access to these logs and associated information is granted under specific conditions to uphold the integrity and security of the College's digital networks and to comply with legal and regulatory requirements.

6.1 Maintenance and Security of Network Activity Logs

The College is committed to the rigorous maintenance of network activity logs, ensuring compliance with the highest standards of privacy and security protocols. These logs systematically record details such as websites visited, email addresses contacted, and the identification of devices initiating these contacts within the College's network infrastructure. The management of these logs is critical for maintaining the integrity and security of our digital networks and for ensuring compliance with prevailing legal and regulatory frameworks.

6.2 Conditions for Access to Information

Access to these detailed logs and associated information is strictly controlled and is permissible under the following specific conditions to safeguard network integrity and comply with statutory obligations:

6.2.1 Triggers During Monitoring

During routine network monitoring, should any anomalies or suspicious activities be detected that indicate potential security threats or violations of policy, designated IST personnel are authorized to access the relevant logs and data. This access is solely for conducting investigations and implementing corrective measures to address such issues.

6.2.2 Internal Investigation Requests

The College may, under circumstances necessitating internal investigations related to compliance with employment policies or following allegations of workplace misconduct, request access to specific network logs and communications. Access under these conditions will be governed by the principles of necessity and proportionality, ensuring it is confined to information pertinent to the investigation at hand.

6.2.3 Lawful Requests from Authorities

Access to network logs may also be granted in response to lawful requests from law enforcement or other governmental authorities. In these instances, the College is committed to full legal compliance, ensuring that any disclosure of information is conducted strictly in accordance with established legal standards and regulatory requirements.

6.3 Compliance and Privacy Obligations

The College acknowledges its legal and ethical obligations to provide access to network records under stipulated circumstances. All procedures related to the access of network information are meticulously designed to balance the need for security with the imperative to protect individual privacy and sensitive information. These procedures are integral to the College's commitment to uphold both legal standards and institutional responsibilities in the management of digital information resources.

ARTICLE 7
Mandatory Cybersecurity Training

7.1 Training Requirements

The College mandates comprehensive cybersecurity training for all staff to strengthen the organization's defenses against cyber threats. This training is designed to equip both employees and students with up-to-date knowledge and skills necessary to protect personal and institutional digital assets.

7.1.1 Annual Refresher Courses

All employees and computer science students are required to participate in annual refresher courses that cover the latest cybersecurity practices, threat awareness, and preventative measures.

7.1.2 Quarterly Phishing Simulations

To enhance phishing awareness and response capabilities, the College will conduct quarterly phishing simulations for all employees. These simulations are critical for testing readiness and providing immediate training for those who inadvertently engage with phishing attempts.

7.2 Compliance and Remediation Pathways

Failure to comply with the cybersecurity training requirements can undermine the College's security posture. Specific remediation paths are established for:

7.2.1 Remediation for Training Non-Completion

Employees and students who fail to complete the mandatory training sessions within the designated time limit will undergo the following steps:

- **Initial Escalation**: Non-compliance will initially be escalated to the individual's manager.
- **Secondary Escalation**: Continued non-compliance will then be escalated to the relevant Service Director.
- **Final Measure**: Persistent non-compliance would lead to escalation to the Director General for appropriate measures to be taken.

7.2.2 Remediation for Phishing Simulation Failures

For those who fall victim to simulated phishing attacks:

- **Immediate Training**: Immediate remedial training will be provided to address specific vulnerabilities.
- **Follow-Up Simulation**: A subsequent simulation will be conducted to ensure effective understanding and application of the training. Further failures may lead to additional training sessions.

7.3 Training Evaluation and Updates

The cybersecurity training program is regularly evaluated for its effectiveness. Feedback from participants is crucial for updating and refining training modules to meet evolving cybersecurity challenges.

7.4 Legal and Ethical Obligations

The College recognizes its legal and ethical responsibilities to enforce robust cybersecurity training. Adhering to these training requirements is essential for maintaining the integrity of both personal and institutional data and for complying with applicable legal standards.

ARTICLE 8
Acceptable Use of Artificial Intelligence (AI)

The use of Artificial Intelligence (AI) tools and platforms on the College's digital networks and devices is authorized only when such use upholds the principles of transparency, accountability, fairness, confidentiality and respect for individual rights. AI use must serve the College's mission and values, comply with all applicable laws and policies, and be conducted in a manner that safeguards personal information, academic integrity, and the reputation of the institution.

8.1 Purpose and Alignment

AI may be used to advance the College's mission in education, research, administration, and innovation. Its use must support student learning and academic success, reinforce the highest standards of academic integrity, and reflect institutional ethics, equity, and inclusion. All AI activities must comply with Quebec legislation, including Law 25 on the protection of personal information.

8.2 Prohibited Uses

The following uses of AI are strictly prohibited:

- **Academic Misconduct:** Using AI to cheat, plagiarize, misrepresent, or otherwise undermine academic integrity, as required by Policy #5 Concerning the Evaluation of Student Achievement..
- **Deception and Disinformation:** Generating or disseminating false, misleading, or harmful content that could damage public trust, the College's reputation, or the integrity of teaching and research.
- **Intellectual Property Violations:** Using AI in ways that infringe upon copyright, trademarks, or other intellectual property rights.
- **Unauthorized Surveillance or Profiling:** Monitoring, profiling, or analyzing individuals without proper consent or legal authorization.
- **Security Breaches:** Employing AI to compromise network security, gain unauthorized access to information, or disrupt College operations.
- **Harassment or Discrimination:** Generating or amplifying content that is harassing, discriminatory, or inconsistent with the College's values of diversity, equity, and inclusion. This includes the creation or dissemination of deepfakes, impersonations, or other forms of synthetic media that could mislead, defame, or cause harm to members of the College community or the public.

8.3 Transparency and Disclosure

When AI use is permitted in a course to assist in the creation of academic or creative work, such use must be clearly disclosed. Students and staff must follow disclosure requirements set out in Policy #5 Concerning the Evaluation of Student Achievement, including proper attribution and acknowledgment of AI contributions. Faculty and administrators are responsible for establishing discipline-specific guidelines on acceptable AI use in academic or operational contexts. Failure to disclose AI use where required constitutes a breach of academic or professional responsibility.

8.4 Privacy and Data Protection

Users must not input personal, confidential, or sensitive College data into public or third-party AI tools, including generative AI chatbots. This includes, but is not limited to, data related to students, employees, academic records, internal operations, or any other information protected under privacy legislation or College policies.

For the purposes of this Policy, and in accordance with Law 25, *personal information* means any information that relates to a natural person and allows that person to be identified, directly or indirectly. This may include names, identification numbers, contact details, biometric or health information, or any combination of data elements that could reasonably identify an individual.

8.5 Accountability

Users are fully responsible for the consequences of their AI use, including the accuracy, reliability, and ethical implications of outputs. Negligent or inappropriate use of AI may result in disciplinary action under College policies, including academic sanctions for students and administrative or employment measures for staff.

8.6 Institutional Use and Tool Approval

The purchase, deployment, or integration of AI tools into College systems, services, or operations requires prior evaluation and approval by the Information Systems and Technology (IST) Service. The IST Service will assess security, compliance, privacy, accessibility, and ethical risks before authorizing institutional AI use. Unauthorized integration of AI into College systems is prohibited.

ARTICLE 9
Inquiries Regarding Policy

All inquiries concerning the implementation, interpretation, or application of this policy shall be formally directed to the Director of IST. The Director of IST is designated as the primary point of contact for addressing any questions or clarifications required by Users of the College's digital networks. This protocol ensures consistent communication and adherence to policy provisions.

ARTICLE 10
Disciplinary Measures

10.1 Reporting and Escalation of Incidents

10.1.1 Incident Reporting

Any Service or department identifying suspected unlawful or prohibited activities within the scope of the digital network must promptly report such instances to the Director of IST. The Director of IST is obligated to assess and document the report and subsequently escalate the issue to the appropriate department for follow-up.

10.1.2 Escalation and Law Enforcement Involvement

Upon receiving a report, the Director General shall evaluate the need for further action, including referral of the matter to appropriate law enforcement agencies for investigation and possible prosecution. This escalation will be undertaken when deemed necessary based on the severity and nature of the infraction.

10.1.3 Corrective Actions

Independently of whether the matter is escalated to law enforcement, the College reserves the right to impose internal measures which may lead to disciplinary actions. Such actions may be initiated regardless of the status or outcome of any criminal proceedings or civil litigation that might ensue from the reported activities.

10.2 Consequences of Policy Violation

Failure to adhere to the present Policy is subject to strict disciplinary actions, which reflect the seriousness of the breach and its impact on the College's operations and reputation. Disciplinary measures may include, but are not limited to:

- **Temporary or Permanent Denial of Network Access:** Users may be denied access to the College's digital networks temporarily or permanently, depending on the severity of the offense.
- **Termination of Employment or Enrollment:** In severe cases, violations of the present Policy may lead to the termination of the User's employment or enrollment at the College. This action will be considered when the violation impacts the College's legal standing, security posture, or breaches trust to a degree that continuation of the employment or academic relationship is untenable.

The College is committed to maintaining a secure and legally compliant digital environment. All members of the College community are expected to cooperate fully with this policy and the procedures established for reporting and handling infractions.

ARTICLE 11
Roles and Responsibilities

11.1 Board of Governors

Board of Governors is responsible for approving the present Policy and subsequent changes to it.

11.2 Director General

The Director General is responsible for the application of the present Policy and any disciplinary measures related to reports of unacceptable or illegal activity.

11.3 Director of Information Systems and Technology (IST)

The Director of IST is responsible for implementing and enforcing the present Policy within the College. This responsibility includes:

- **Policy Enforcement**: Establishing and maintaining robust College practices to ensure ongoing compliance with the present Policy.
- **Investigations**: Overseeing investigations into any reports of unacceptable or unlawful activities conducted by users of the College's digital networks. This includes coordinating with other Services or departments or external agencies as necessary to address and resolve such issues effectively.
- **Principles and Goals**: Setting the overarching principles and goals of the present Policy, ensuring that it supports the College's strategic objectives and compliance with all applicable laws and regulations.

The Director of IST is responsible for the ongoing review and revisions to the present Policy to ensure its continued relevance and effectiveness. The review process shall occur as needed based on evolving legal, technical, and operational considerations, or at a minimum, triennially from the date of its enactment. Revisions will be undertaken to address developments in technology, changes in legal requirements, or procedural efficiencies.

11.4 Senior Managers

Senior Managers within the College are entrusted with specific responsibilities to uphold the integrity of the present Policy:

- **Awareness and Education**: Ensuring that all Users within their respective Services or departments are fully informed about the present Policy, understand its implications, and are aware of the consequences of non-compliance.

- **Security Screening**: Overseeing the security screening processes to ensure that all Users have appropriate clearance and authorization before accessing sensitive systems, networks, or applications.
- **Access Termination**: Facilitating the prompt termination of network access for individuals who are no longer employed by or affiliated with the College, thereby protecting sensitive information and resources from unauthorized use or access.

11.5 Compliance and Effectiveness Assessment

Senior Management must assess compliance with the present Policy and its effectiveness in the College's annual planning process. This assessment is crucial for identifying areas of improvement and ensuring that the present Policy remains effective in managing the risks associated with digital network usage.

11.6 User Responsibilities

11.6.1 Obligation to Comply

Compliance with the present Policy is compulsory for all students, employees, contractors, and any other individuals granted authorization to operate within the College's digital network. This requirement extends to any party engaging with or using digital networks under the auspices of the College.

11.6.2 Familiarity and Acknowledgment

Each User must acquaint themselves with the stipulations of the present Policy before accessing the College digital networks. To this end, everyone must:

- **Policy Familiarization**: Undertake to understand the scope, provisions, and implications of the present Policy as it pertains to their roles and responsibilities within the College.
- **Mandatory Acknowledgment**: Complete and sign the "User Agreement Form" (Reference Document #P23.1), which is obtainable through the College's Information Systems and Technology Service. This form serves as a formal acknowledgment of the User's comprehension and acceptance of the present Policy, affirming their commitment to adhere to its guidelines and restrictions each time the network is accessed.

ARTICLE 12
Revisions

The present Policy will be reviewed every five (5) years or when deemed necessary.

GLOSSARY

Acceptable activity:	This implies use by students, employees, each administrative service, academic program, and other authorized individuals for conducting business on behalf of the College (refer to article 4.1).
Artificial Intelligence:	Refers to systems, software, or technologies that perform tasks typically requiring human intelligence. These tasks may include learning, reasoning, problem-solving, decision-making, language understanding, or content generation.
College community:	The term used includes staff, students, parents, the Board of Governors, and individuals or organizations with whom the College has a working or service relationship on or off College premises.
Deepfake:	Refers to any image, audio, or video content that has been synthetically generated or altered using artificial intelligence or machine learning techniques to falsely depict a person saying or doing something they did not actually say or do.
Digital networks:	Groups of computers and computer systems that can communicate with each other. Without restricting the generality of the foregoing, these networks include the Internet, networks internal to the institution and public and private networks external to the institution.
Hacking:	This refers to the practice of exploiting weaknesses in a computer system, network, application, or digital device to gain unauthorized access, perform malicious activities, or manipulate the system's behavior.
Monitoring:	The recording and analyzing of the information and control transactions that take place on digital networks.
Personally Identifiable Information (PII):	Refers to any information that can directly or indirectly identify an individual. This includes both direct identifiers (e.g., full name, social insurance number, student ID number, driver's license number, email address, phone number) and indirect identifiers that, when combined, could reveal an individual's identity (e.g., date of birth, postal code, gender, or other demographic details).
Prohibited activity:	This includes criminal offenses, contraventions of non-criminal regulatory federal and provincial statutes, and actions that make a student or an employee, an authorized representative or all administrative services and academic departments liable to a civil lawsuit and/or criminal proceedings (refer to article 4.2 and 4.3).
User:	Any individual or entity that interacts with a computer system, software application, network, or digital service.

Related Documents

This document is to be used in conjunction with:

- *Charter of Human Rights and Freedoms (CQLR, c C-12)*[1]
- *Act respecting the governance and management of the information resources of public bodies and government enterprises (CQLR, c G-1.03)*[2]
- *Act respecting Access to documents held by public bodies and the Protection of personal information (CQLR, c A-2.1)*[3]
- CÉGEP Heritage College Code of Ethical Conduct[4]
- CÉGEP Heritage College Policy #48 Concerning Personal Information and Confidentiality[5]
- CÉGEP Heritage College Policy #6 Concerning a Respectful Workplace Free of Discrimination and Harassment[6]
- CÉGEP Heritage College Policy #5 Concerning the Evaluation of Student Achievement[7]
- CÉGEP Heritage College Policy #22 Concerning Records and Archives Management[8]
- CÉGEP Heritage College Policy #24 Concerning Standards of Student Conduct[9]
- CÉGEP Heritage College Procedures #40 Concerning Safe Disclosure[10]

[1] Copies of this document are available from the Director General's Office.
[2] *Ibid*.
[3] *Ibid*.
[4] Copies of this document are available from the Director General's Office and on the College Website.
[5] *Ibid*.
[6] *Ibid*.
[7] *Ibid*.
[8] *Ibid*.
[9] *Ibid*.
[10] Copies of this document are available from the Director General's Office and on Heritage Employees Team.

Reference Documents

- Reference Document #P23.1 – Student User Agreement Form
- Reference Document #P23.2 – Employee User Agreement Form
- Reference Document #P23.3 – Exemption Authorization Form (Employees)