

**HERITAGE COLLEGE
POLICY #23**

**CONCERNING THE USE OF
ELECTRONIC NETWORKS**

ADOPTION AND REVISION

The present Policy was adopted on September 28, 1999

Most recent date of revision:

HERITAGE COLLEGE POLICY #23

CONCERNING THE USE OF ELECTRONIC NETWORKS

ARTICLE 1

Preamble^{1 2}

Access to the Heritage College electronic networks is provided as a resource for students and employees to support attainment of the College mission and overall educational objectives. By encouraging effective and innovative use of the College electronic networks within Heritage College, students and employees will be able to explore new avenues of communication, share information with colleagues and the public, reach out to wide audiences to spread sustainable development messages, and foster better public education. One of these networks, the Internet, is a vast and rapidly growing system that links millions of computer users around the world. This linkage enables Internet users to access and easily share a wealth of information on an increasingly wide variety of topics throughout the world. The College electronic networks, therefore, represent a valuable resource for Heritage College, its students and its employees, for research and technical information, communication, public relations and overall College visibility. As such, these networks are a key instrument for the facilitation of learning and student success in this College.

Although the College electronic networks represent a valuable resource, they also expose Heritage College and individuals to potential harm if not used appropriately. Therefore, all aspects of the College electronic networks must be carefully managed to ensure that the Heritage College image is properly protected, that legal risks are minimized and that access and use of departmental electronic networks by Heritage College employees, students and other authorized individuals are suitable for College purposes.

¹Relevant Legislation: The *Financial Administration Act*; the *Access to Information Act*; the *Privacy Act*; the *Charter of Rights and Freedoms*; the *National Archives of Canada Act*; the *Official Secrets Act*; the *Criminal Code*; the *Exports and Import Act*, the *Crown Liability and Proceedings Act*; the *Copyright Act*; the *Trade-Marks Act*; the *Patent Acts*; the *Canadian Human Rights Act*.

² See the Glossary for explanations of frequently-used terms.

ARTICLE 2

Purpose

The purpose of this policy is to clearly communicate Heritage College expectations of acceptable use of the departmental electronic networks, and to provide information about and examples of unacceptable or unlawful activity, which is not permitted. Its purpose is to ensure that departmental business is not compromised due to deliberate misuse of the departmental electronic networks and to protect Heritage College against legal risks caused by deliberate misuse.

ARTICLE 3

General Provisions

Use of the Heritage College electronic networks by students, employees or others (as defined under *article 4.0*) is permitted for conducting business related to academic departmental programs and College services, and for personal use (only when such use is on personal time), is not for financial gain, and does not add to Heritage College costs. As such, the College electronic networks are to be used in a manner consistent with this policy. Any violations of this policy will not be tolerated and will be dealt with quickly, fairly and decisively.

ARTICLE 4

Application

This policy applies to all Heritage College students, employees and others who have been provided a departmental account to access the electronic networks, including specified period employees, contract workers³ and volunteers. It extends to situations away from the workplace such as telework or remote access, including home PCs, during or outside working hours, where access to the departmental electronic networks is used.

³Contractors can, with Heritage College management approval, access the departmental electronic networks for Heritage College related purposes to the extent needed to complete a stated assignment. Where access to the departmental electronic networks is required it will be included in the terms and conditions of the contract, including an acknowledgment of this policy.

HERITAGE COLLEGE POLICY #23
CONCERNING THE USE OF ELECTRONIC NETWORKS

ARTICLE 5
Requirements

5.1 Acceptable Activity

The following examples of “acceptable activity” using the departmental electronic networks include, but are not limited to:

- conducting one’s work according to one’s accountability and mandate at Heritage College;
- communicating and sharing non-classified or non-designated work-related information with public service professionals, the public, and professional contacts;
- obtaining computer programs or non-commercial software to augment certain business tasks;
- supporting one’s career development;
- making personal use on personal time as long as such use is in compliance with this policy;
- making use of the Internet for any of the above activities.

Furthermore, Heritage College employees are permitted to create individual home pages that must relate to departmental programs and services; pre-authorization must be obtained from the Director General's office and must be registered with the sector Webmaster.

5.2 Unacceptable Activity

Unacceptable activity is prohibited. The following examples of “unacceptable activity” on the departmental electronic networks in violation of Heritage College policies include, but are not limited to:

- sending classified or designated information on unsecured networks, unless it is sent in encrypted form;
- accessing sensitive information without authorization;
- causing congestion and disruption of networks and systems through such means as sending chain letters and subscribing to list server electronic mail unrelated to a work purpose;

- sending abusive, sexist or racist messages to employees and other individuals;
- making excessive public criticisms of governmental policy;
- representing personal opinions as those of Heritage College;
- attempting to defeat information technology security features through such means as using someone else’s password, user-identification or computer account; or disclosing one’s password, network configuration or access codes to others;
- adding or downloading computer games;
- making use of the Internet for any of the above activities, including intentionally interfering with the normal operation of any departmental Internet gateway or using the Internet for private business, personal gain or profit, or political activity.

Furthermore, it is an “unacceptable activity” to use the departmental electronic networks to access or download web sites or files, or to send or knowingly receive electronic mail messages or other types of communication:

- that incite hatred against identifiable groups contained in personal messages; or
- whose main focus is pornography, nudity, and/or sexual acts;
- in order to add or download computer games.

5.3 Unlawful Activity

Unlawful activity is prohibited. For the purpose of this policy, “unlawful activity” is interpreted broadly to include actions that could result in sanctions of different kinds in a court of law, which includes criminal offences or failure to observe statutory requirements. Each department has a responsibility to report suspected illegal activity, to the Coordinator of Computer Services.

The following examples of “unlawful activity” on the departmental electronic networks considered as “criminal offences” include, but are not limited to:

HERITAGE COLLEGE POLICY #23
CONCERNING THE USE OF ELECTRONIC NETWORKS

- possessing, downloading or distributing any pornography;
- infringing on another person's copyright without lawful excuse;
- causing a statement to be read by others which is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person;
- sending electronic messages, without lawful authority, that cause people to fear for their safety or the safety of anyone known to them;
- disseminating messages that promote hatred or incite violence against identifiable groups;
- distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material;
- hacking and other crimes related to computer security which include: gaining unauthorized access to a computer system; trying to defeat the security features of the electronic networks; spreading viruses with the intent to cause harm; destroying, altering or encrypting data without authorization and with the intent of making it inaccessible to others with a lawful need to access it; and interfering with others' lawful use of data and computers;
- making use of the Internet for any of the above activities including: downloading pornography, publishing obscene material, or various other offences such as fraud, extortion, bribery or illegal gambling.

The following examples of "unlawful (though not *criminal*) activity" on the departmental electronic networks in violation of federal and provincial statutes include, but are not limited to:

- violating another person's copyright or unauthorized use of trademarks and patents;
- uploading or downloading commercial software in violation of its copyright;
- spreading false allegations or rumors that would harm a person's reputation;

- disclosing sensitive information without authorization which includes disclosing personal information, business trade secrets, or sensitive government information;
- unlawfully destroying, altering or falsifying electronic records;
- privacy infractions such as reading someone else's e-mail or intercepting e-mail in transit;
- making use of the Internet for any of the above activities including: violating another person's copyright, disclosing or collecting personal information without authorization, or posting inaccurate information that causes harm or results in damages.

ARTICLE 6 Responsibilities

6.1 User Responsibilities

- 6.1.1 Adherence to this policy is mandatory for all Heritage College students and employees, as well as contractors and other persons authorized to work on behalf of a department, who access the departmental electronic networks.
- 6.1.2 Each user is responsible for becoming familiar with this policy and adhering to it every time they access the departmental electronic networks. All users will be required to read and sign the "User Agreement Form" (*Reference document #P23.1*) available from Computer Services.

6.2 Management Responsibilities

- 6.2.1 The Coordinator of Computer Services is responsible for establishing and maintaining departmental practices required to verify adherence to this policy.

The Coordinator of Computer Services is responsible for investigating, or coordinating the investigation of, reports of

HERITAGE COLLEGE POLICY #23
CONCERNING THE USE OF ELECTRONIC NETWORKS

unacceptable or unlawful activity by Heritage College users.

- 6.2.2** All senior managers are responsible, in their respective areas, for ensuring users' awareness and understanding of the requirements of this policy to ensure:
- that they do not violate the policy through lack of understanding;
 - that users are properly security screened for access to systems, networks, or applications used to process sensitive information; and
 - the termination of a user's access to the departmental electronic networks in the event that that individual is no longer employed by, or affiliated with, the College.
- 6.2.3** The senior management team, as part of its annual planning process, assesses the need to review and report on compliance with this policy and the effectiveness of its implementation.
- 6.2.4** The Director General will develop a clause for the *Articles of Agreement* in the Heritage College contract document that will ensure contractors' awareness and adherence to this policy.

ARTICLE 7 Disciplinary Measures

- 7.1** A department will report suspected unacceptable or illegal activity to the Coordinator of Computer Services, who will bring the matter to the attention of the Director General. The Director General will refer the matter to the appropriate law enforcement agency, if necessary. The College may take disciplinary action even if a criminal charge or civil lawsuit is not pursued.

- 7.2** Failure to comply with this policy could result in disciplinary action ranging from denial of access up to and including termination of employment or studies at the College.

ARTICLE 8 Monitoring

Heritage College has an obligation to ensure compliance with this policy, along with other departmental and College policies. Because of this obligation, it must be recognized that some monitoring of the departmental electronic networks is required. The departmental electronic networks are routinely monitored for operational reasons, which is necessary to assess system or network performance, protect College resources, and ensure compliance with College policies.

For the purpose of this policy, an analysis of usage logs will take place on an *ad hoc* basis — as a result of a complaint, when there is a reasonable expectation of unacceptable or unlawful activity, or when obvious anomalies appear during routine monitoring practices for operational reasons. Any resulting investigation will be conducted in accordance with the *Charter of Rights and Freedoms*, the *Privacy Act* and the *Criminal Code*.

ARTICLE 9 Access to Information

Departmental users should be aware that the firewalls, gateways and systems record which web sites and electronic mail addresses were contacted and which computer within a department made the visit or sent the message. The College could find itself under legal obligation to provide access to these records.

ARTICLE 10 Enquiries

Enquiries about this policy are to be directed to the Coordinator of Computer Services.

ARTICLE 11 Coming into Force and Revision

HERITAGE COLLEGE POLICY #23
CONCERNING THE USE OF ELECTRONIC NETWORKS

This policy comes into force upon its adoption by the Board, and will be revised by the Coordinator of Computer Services as required or at least every three years after its adoption.

HERITAGE COLLEGE POLICY #23
CONCERNING THE USE OF ELECTRONIC NETWORKS

GLOSSARY

- Acceptable activity:** This implies use by students, employees, each administrative service, academic program and other authorized individuals for conducting business on behalf of Heritage College (*refer to article 5.1*).
- Electronic 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.
- Monitoring:** The recording and analyzing of the information and control transactions that take place on the electronic networks.
- Unacceptable activity:** Any activity that violates Heritage College policies (*refer to article 5.2*).
- Unlawful activity:** This includes criminal offences, 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 5.3*).