

SCHEDULE "A"

1 POLICY ON THE USE OF ELECTRONIC NETWORK

1.1 Preface

Use of The Town of Bancroft electronic network / equipment (E-mail, Intranet, Internet access, etc.) is provided as an information tool for employees and other authorized individuals to support the attainment of The Town of Bancroft's mandate. This tool is meant to assist authorized users by expediting the transfer of data and information to The Town of Bancroft's partners and clients, and by providing access to the information authorized users need to do their jobs. The network is a finite resource, which must be used responsibly to maintain its integrity. Municipal values should guide your use of our network /equipment.

1.2 Application

This policy applies to all Municipal employees and to other authorized users who are provided with access to The Town of Bancroft's electronic network / equipment.

1.3 Policy Objective

To ensure that the appropriate use of the electronic network / equipment by authorized users by defining corporate expectations with respect to the use of the electronic network / equipment to minimize risk of unacceptable and unlawful behaviour.

1.4 Policy Statement

It is the policy of The Town of Bancroft that authorized users may use The Town of Bancroft electronic network / equipment for authorized uses only.

1.5 Policy Requirements

1.5.1 Authorized Uses of the Electronic Network / Equipment

Authorized users are permitted use of the electronic network / equipment: to fulfill work responsibilities and further The Town of Bancroft mandate; for career development; and for personal use that: - is on personal time; is not for financial gain; does not add to The Town of Bancroft's costs; and does not interfere with the conduct of Municipal business.

1.5.2 Responsibilities

Adherence to applicable policies and guidelines as set out by The Town of Bancroft is mandatory for all authorized users of the electronic network /equipment.

1.5.2.1 *Authorized users are responsible for:*

- *taking reasonable measures to control the use of their password, user identification and computer accounts;*
- *following instructions to ensure network and information security; using departmentally provided security features to avoid transferring computer viruses;*
- *writing communications accurately and clearly, in a professional manner, so that our use of the electronic network will reflect well on The Town of Bancroft; ensuring their communications about policies, programs and services are accurate and clear, and comply with Municipal policies;*
- *avoiding unlawful activity that could result in sanctions of different kinds in a court of law (criminal charges or civil lawsuits) (e.g. defamation, harassment, obscenity, child pornography);*
- *avoiding unacceptable activity that may not be unlawful but that violates departmental Municipal policies (e.g. abusive or sexist messages);*
- *contacting their manager when in doubt about proper usage procedures and practices.*

Authorized users should be aware of any departmental information technology systems guidelines when posting information to the Internet/Intranet, or through E-mail. Authorized users should also be aware that anything posted on the Internet/Intranet, internal and Internet E-mail, as well as departmental logs of Internet sites visited by individuals, are accessible under the Municipal Freedom of Information Act as well as the Privacy and Access to Information Acts. Any information requested under these acts will be reviewed and exemptions invoked where applicable to protect information such as personal information about employees or clients. The contents of all messages may be used and disclosed for any purposes without the authorization of the originator or recipient. Users should not post any sensitive information on the Intranet/Internet or E-mail prior to ensuring the proper security measures are in place and/or that the information would not qualify for exemptions under the aforementioned acts.

1.5.2.2 **Managers** are responsible for ensuring authorized users in their area are aware of this policy. Managers are required to deal with all suspected violations of this policy. The decision as to what extent the electronic network is required for a particular job rests with the Department Head.

More specifically, Department Heads and managers should:

- *ensure that all authorized users in their area have the necessary information on unacceptable and unlawful uses of the departmental electronic network;*
- *and ensure that all reports of unacceptable or unlawful use by authorized users are investigated an appropriate corrective action is taken.*

1.5.3 **Unacceptable and Unlawful Conduct/Activity**

1.5.3.1 **Unacceptable** activities are those which violate departmental guidelines as well as departmental and Municipal policies. Examples include; causing congestion and disrupting networks and systems, downloading sensitive data or client database information without proper authorization, destroying or altering data without authorization, and sending abusive, sexist or racist messages to employees and other individuals (for a non exhaustive list of examples see section 52-8).

1.5.3.2 **Unlawful** activities include criminal actions that violate the Criminal Code of Canada and those federal or provincial statutes that provide for criminal offences. It also includes those activities that violate non-criminal, regulatory statutes. When an employee performs an activity in the course of his or her employment which results in lawsuits brought by persons harmed by that activity, both the employee and the employer can be held liable for these actions. Examples include; copyright infringement, defamation, obscenity and child pornography (for a non-exhaustive list of unlawful activities, see section 1-9).

1.5.4 **Monitoring of the Electronic Network**

The Town of Bancroft electronic network will be monitored to protect government resources and/or ensure compliance with this policy. All traffic originating or terminating in our network is recorded. The Town of Bancroft may conduct periodic and random checks of the network for operational purposes. In such cases, The Town of Bancroft may analyze the resulting information. A routine analysis does not involve reading the content of electronic mail or files.

Regular monitoring of the electronic network will be undertaken in a manner that strikes a balance between protecting the privacy rights of the individual and facilitating the necessary and appropriate auditing and review for unacceptable and unlawful usage.

If due to a routine analysis or a complaint, The Town of Bancroft reasonably suspects that a user is misusing the network, special monitoring without prior notice will occur. All investigations will be undertaken in accordance with the Charter of Rights and Freedoms, the Privacy Act, and the Criminal Code. Internal audits will be conducted to ensure compliance with this policy and the effectiveness of its implementation.

**By-Law No. 22-2015
Schedule "A"**

1.5.5 Sanctions Against Abuse

Suspected unlawful activity will be reported to law enforcement authorities, unless the Department Head in consultation with The Town of Bancroft Administrator and Legal Services determine that the matter is a minor one and can be dealt with administratively. The Town of Bancroft may take disciplinary measures, even where a formal criminal charge or civil lawsuit is not pursued.

Unacceptable, unlawful or unauthorized use of the electronic network could result in disciplinary action being taken against a user as appropriate. Discipline could range from an oral or written reprimand up to and including termination of employment.

1.6 Inquiries

For inquiries:

- concerning the intent and implementation of this policy contact your Department Head.
- concerning monitoring, contact the CAO.
- relating to security, privacy and access to information contact your immediate Supervisor.

1.7 Definitions

For the purpose of this policy, the following definitions apply:

- 1.7.1 **Access** means gaining entry to an electronic network that The Town of Bancroft has provided to authorized individuals. Access to such networks may be from inside or outside Municipal premises. Access may support telework and remote access situations or where authorized individuals are using electronic networks provided by The Town of Bancroft on their own time for personal use.
- 1.7.2 **Authorized users** include managers and employees of The Town of Bancroft as well as other persons such as contractors and students who have been authorized by the Department Head to access The Town of Bancroft's electronic network.
- 1.7.3 **Electronic networks** are 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 Town of Bancroft, and public and private networks external to The Town of Bancroft.
- 1.7.4 **Monitoring of electronic networks** means any action that involves the recording and subsequent analysis of activity on, or use of, a system or electronic network. Examples include recording user accounts, user activities, sites visited, information downloaded and computer resources used to perform a routine analysis of traffic flow on networks, use patterns and sites that certain work groups or individuals have visited. The information recorded and subjected to analysis does not normally involve the contents of individual electronic mail, files and transmissions.
- 1.7.5 **Personal time** includes breaks, lunchtime and the time before and after work. It is the policy of The Town of Bancroft that authorized users may use The Town of Bancroft electronic network for authorized uses only.
- 1.7.6 **Unacceptable activity** is any activity that violates Municipal policy or that violates the limitations on personal use (see section 1-8 for examples).
- 1.7.7 **Unlawful activity** includes criminal offences, contravention of noncriminal regulatory federal and provincial statutes, and actions that make an authorized individual or The Town of Bancroft liable to a civil lawsuit (see section 1-9 for examples).

1.8 Examples of Unacceptable Activity on Electronic Networks

A number of Municipal and Provincial policies apply whether the unacceptable activity occurs on paper, by telephone, through the electronic network, in oral conversation or through any other medium. It is unacceptable to violate Municipal and Provincial policies. The following are examples:

**By-Law No. 22-2015
Schedule "A"**

- 1.8.1 **Accessing, without authorization, sensitive information held by the government.** It is unacceptable to download sensitive data or client database information without proper authorization.
- 1.8.2 **Attempting to defeat information technology security features,** through such means as using anti-security programs; using someone else's password, user-identification or computer account; disclosing one's password, network configuration information or access codes to others; or disabling anti-virus programs.
- 1.8.3 **Causing congestion and disruption of the network and systems,** through such means as sending chain letters and receiving list server electronic mail unrelated to work purposes. These are examples of excessive use of resources for non-work related purposes.
- 1.8.4 **Failing to revoke system access rights for personnel when they leave the institution or when they lose their reliability status or security clearance.**
- 1.8.5 **Making excessive public criticisms of Municipal or government policy.**
- 1.8.6 **Providing authorized users with access to systems, networks, or applications used to process sensitive information before they are authorized by the Department Head.**
- 1.8.7 **Representing personal opinions as those of The Town of Bancroft, or otherwise failing to comply with Municipal or departmental procedures concerning public statements about The Town of Bancroft's positions.**
- 1.8.8 **Sending abusive, sexist or racial messages to other employees and other authorized individuals.**
- 1.8.9 **Sending classified or designated information on unsecured networks,** unless it is approved by the Department Head and sent in an approved encrypted form.
- 1.8.10 **Unauthorized removal or installation of hardware or software** on Municipal owned informatics devices or electronic networks.
- 1.8.11 **Using The Town of Bancroft's electronic networks for private business, personal gain or profit or political activity.**
- 1.8.12 **Access, download, send or receive documents whose main focus is pornography, nudity or sexual acts or documents that incite hatred against identifiable groups contained in personal messages.**

1.9 **Examples of Unlawful Activity on Electronic Networks**

For the purpose of this policy, "unlawful activity" is interpreted broadly to include actions that could result in sanctions of different kind in a court of law.

1.9.1 **Violations of the Criminal Code of Canada**

The following are examples of criminal activity:

- 1.9.1.1 **Child pornography:** *possessing, downloading or distributing any child pornography.*
- 1.9.1.2 **Copyright:** *infringing on another person's copyright, without lawful excuse (see also "copyright" under section 1-9-2.1).*
- 1.9.1.3 **Defamation:** *causing a statement to be read by others that is likely to injure the reputation of any person by exposing them to hatred, contempt or ridicule, or that is designed to insult the person.*
- 1.9.1.4 **Hacking and other crimes related to computer security:** *Gaining unauthorized access to a computer system. Trying to defeat the security features of the electronic network. Intentionally spreading viruses with intent to cause harm. Destroying, altering or encrypting data without authorization and with intent of making it inaccessible to others with a lawful need to access it. Interfering with others' lawful use of data and computers.*
- 1.9.1.5 **Harassment:** *sending electronic messages that cause people to fear for their safety or the safety of anyone known to them and sending threats to cause serious bodily harm, damage personal property or injure a person's animal.*
- 1.9.1.6 **Hate propaganda:** *disseminating messages that promote hatred or incite violence against identifiable groups in statements outside private conversations.*
- 1.9.1.7 **Interception of private communications or electronic mail (in transit):** *unlawfully intercepting someone's private communications or unlawfully intercepting someone's electronic mail.*
- 1.9.1.8 **Obscenity:** *distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material.*

By-Law No. 22-2015
Schedule "A"

1.9.1.9 *Various other offences: these include, fraud extortion, blackmail, bribery, illegal gambling and dealing in illegal drugs can occur, in whole or in part, over the electronic network.*

1.9.2 **Violations of Federal and Provincial Statutes**

The following are examples of unlawful (though not criminal) activity:

1.9.2.1 **Copyright and intellectual property:** *violating another person's copyright and unauthorized use of trademarks and patents.*

1.9.2.2 **Defamation:** *spreading false allegations or rumours that would harm a person's reputation.*

1.9.2.3 **Destroying or altering data without authorization:** *unlawfully destroying, altering or falsifying electronic records.*

1.9.2.4 **Disclosing sensitive information without authorization.**

- *Disclosing personal information.*
- *Disclosing business trade secrets.*
- *Disclosing sensitive Municipal information.*

1.9.2.5 **Harassment:** *discriminating against an individual on the basis of; race, national or ethnic origin, colour, religion, age, sexual orientation, marital status, family status, disability and conviction for which a pardon has been granted. Thus, in some circumstances, displaying unwelcome sexist, pornographic, racist or homophobic images or text on a screen at work can be unlawful harassment.*

1.9.2.6 **Privacy infractions:** *reading someone else's electronic mail or other personal information without authorization or intercepting electronic mail while it is in transit.*

1.9.2.7 **Use of public money without proper authority:** *offences include making a requisition without authority, taking bribes or participating in corrupt practices.*

1.9.3 **Activity that can Expose Authorized Individuals or The Town of Bancroft to Civil Liability**

The following are examples of civil wrongs:

1.9.3.1 **Disclosing or collection of sensitive data:** *revealing or obtaining such information without authorization.*

1.9.3.2 **Defamation:** *spreading false allegations or rumours that would harm a person's reputation.*

1.9.3.3 **Inaccurate information:** *posting inaccurate information, whether negligently or intentionally.*