

## **POLICY STATEMENT AND PURPOSE**

The County of Elgin provides employees, elected officials, and other organizations and individuals with access to computer and network services including internet use and email for business purposes.

Access to the Internet enables authorized users to research and obtain information relevant to County business; and to provide information to residents, potential residents, businesses and business prospects of the County of Elgin.

This Policy outlines the County's expectations regarding computer usage and sets clear parameters for authorized users to ensure clarity surrounding the use of this corporate resource.

Authorized users are expected to practice good judgment and to demonstrate a sense of responsibility and consideration of others, when using the County's network and services. All work undertaken shall be performed in an ethical and lawful manner, demonstrating integrity and professionalism by all users.

## **SCOPE**

This policy applies to all authorized users of the County's computer and network services, including but not limited to: County employees and elected officials, (including temporary and contract employees, volunteers, students and interns) and other authorized organizations or individuals.

## **ACCESS**

All authorized users have access to the County's network, including internet access and email.

## **Privacy**

The County of Elgin respects the privacy of employees. However, any electronic record created on a County computer or sent through the County network is considered to be the property of the County of Elgin.

## **USAGE**

The primary use of the County's computer and network services is for business purposes. Limited, occasional or incidental use of the County's network for personal activities are acceptable, provided the privilege is not abused.

Authorized users shall conduct email messaging in the same manner as they would other business correspondence, being mindful of the fact that email transmissions over the Internet are not secure and may be intercepted, and that email is subject to the provisions of The Municipal Freedom of Information and Privacy Act. Authorized users are responsible for all email sent from their individual user name, and should take appropriate precautions to ensure that their password is not shared with anyone, except within the terms of this policy.

The following restrictions apply:

- No information should be distributed on the Internet, which would not be distributed under the County's letterhead or logo. Material which is viewed, copied, downloaded or saved should be primarily related to County business. (Refer to auditing section of this policy)
- Authorized users shall not install or run security programs or utilities which reveal weaknesses in the security of a system, whether internal or external to the County's network. Users shall not, in any way, attempt to access unauthorized/confidential information to which they have not been previously granted access.

- 
- Information which would not be distributed to members of the public such as draft reports, confidential information or information which is restricted under the Municipal Freedom of Information and Personal Privacy Act, etc., may not be entered on the Internet or sent by email unless it is properly protected, and its distribution has been properly authorized.
  - Employees must comply with copyright and licensing restrictions on any information which has been downloaded.
  - Any acquisition of goods or services must be in accordance with the County's Purchasing By-law. Authorized users may not offer goods or services over the Internet on the County's network for personal use, nor may they send "for sale or wanted to buy" messages on the Internet or by email.
  - Authorized users must abide by vendor license agreements. Use of applications and/or data is subject to the license agreement and may not be reproduced in any form without permission from the Vendor.
  - Data originating on the County network is owned by the County and may not be distributed outside the County without proper authorization from the owner or custodian of the data.

***Acceptable and appropriate Internet and email use includes but is not limited to:***

1. Participating in professional, job-related research
2. Distributing work-related correspondence, minutes, agendas, reports, etc.
3. Communicating with staff, official bodies and vendors.
4. Responding to public inquiries.
5. Accessing job-related distance learning opportunities.
6. Creating job-related information resources.
7. Participating in job-related list serves or mailing lists.
8. Communicating with staff, elected officials, and appropriate outside bodies such as other levels of government, businesses, County partners, citizen groups and residents.

---

***Unacceptable and inappropriate Internet and email use includes, but is not limited to the following list. The only exception is in performance of work related matters as approved by Directors or their designates.***

1. Sending emails to “all users” must receive prior authorization from a department director before being sent.
2. Participating in Internet Chat groups, or list serves that are not work related.
3. Accessing sites or transmitting material which violates any Canadian federal or provincial law or County by-law or directive, such as defamatory, discriminatory or obscene material, and sites or tools dedicated to computer/network hacking, or sites which in the opinion of management are inappropriate.
4. Accessing, displaying or storing (on the County’s network) fraudulent, harassing or obscene email messages; or email messages, graphics or images which are offensive and conducive to a poisoned work environment. \*
5. Storing games, game-related data, or personal web site material on any network
6. Installation and use of software and applications *banned* by Information Technology, including but not limited to: Kaza, Morpheus LimeWire, Donkey 2000, Bear Share, Gnutella, Nutella, iMesh, Blubster. Instant Messaging applications – AIM (AOL Instant Messenger), ICQ, NET, MSN or Windows Messenger, Yahoo Messenger Services.
7. Downloading or storing MP3 files.
8. Sending chain letters and sending junk mail (spamming) or broadcast transmissions (i.e.) sending a single message to a large number or individual email addresses.
9. Using Internet web-based email systems such as Hotmail, Yahoo, etc. from within the County’s network.
10. Sending anonymous messages or accessing the Internet under another person’s network identification without such person’s permission.
11. Allowing others who are not authorized users to access and utilize County equipment or software.
12. Sharing County account or passwords with any other person (including family members), except as authorized in writing by Directors.
13. Making unauthorized copies of copyrighted software. It is the responsibility of individual departments to ensure they obtain the appropriate software licensing and the responsibility of authorized users to obtain appropriate licensing for home units.

14. Changing the configuration of County computers through the use of unauthorized boot disks, circumventing County computer security measures, attempting to gain access to a County system for which proper authorization has not been given or probing the security at any computer site, internal or external to the County.
15. Authorized users not logging off their computers at the end of each day or when leaving the workplace for any extended period.

\* Inadvertently accessing an inappropriate site or receiving an email with an unacceptable attachment, will **not** be considered a violation of this policy. Printing, saving or forwarding inappropriate material (except as properly authorized) shall be considered a violation of this policy.

## **DEFINITIONS**

**Access:** gaining entry to a network provided by the County to its employees and other authorized users, on or outside County premises, including telework situations and where employees or authorized users are using the network for business purposes or for personal use in accordance with the provisions of this policy on their own time.

**Authorized Users:** Persons using a computer or computer account in order to perform work in support of County business.

**Boot disks:** Diskettes used to load a computer's operating system, or "boot up" the computer.

**Data:** Any formalized representation of facts, concepts or instructions suitable for communication, interpretation or processing by a person or by automatic means.

**Instant Messaging:** an internet communications service used to send and deliver messages and content immediately. To use the service, users must be logged on to the server that hosts the instant messaging service, e.g. private chat room

**Internet:** The internet is a world-wide collection of networks which is linked through a common communications protocol and which collection of networks is used as a common basis for communications for all types of applications. Use of the Internet specifically includes access to the World Wide Web (WWW).

**List serves:** An automated mailing list distribution system that allows users to add or delete themselves from mailing lists without human intervention.

**Network:** computers and computer systems which can communicate with each other and without restricting the generality of the foregoing, including the internet, networks internal to an institution, as well as closed networks external to an institution.

**Telework:** Work involving paid staff, undertaken away from the normal place of work, often known as working from home or telecommuting.

**Vendor License Agreement:** Contract or other document delineating the terms of the software or data use arrangements with the seller/manufacturer.

#### **RELEVANT LEGISLATION:**

The Municipal Freedom of Information and Protection of Privacy Act:  
The Purchasing By-law of the County of Elgin  
The Ontario Human Rights Code  
The Copyright Act  
The Criminal Code of Canada

#### **ADMINISTRATION:**

This policy is administered by the Information Technology Department

**AUDITING:** All Authorized Users should be aware that the County's network creates records of every Internet site visited and every message sent by email. If abuse of the County's system, or contravention of this policy is suspected, Directors or their designates may request an audit of the Authorized user's operation of the system.

**COMPLIANCE:** Failure to comply with this policy may result in appropriate discipline measures up to and including dismissal.

**CONTACT:** For more information or procedures, contact Information Technology Department.

## **ELECTRONIC COMMUNICATION RETENTION POLICY**

### **Policy Scope**

This policy governs the retention of electronic communications within the County of Elgin. For the purposes of this policy, electronic communications includes electronic mail, text messaging and voice mail which are defined as follows:

*Electronic mail:* The transmission of typed messages and/or attached documents of unlimited length over an electronic telecommunications network that can be read and replied to using either a personal computer or hand-held device.

*Text messaging:* The transmission of short, textual messages over a telecommunications network that can be read and replied to using a portable phone, pager, personal digital assistant, or other handheld device.

*Voice mail:* The transmission of verbal messages sent over a telecommunications network stored in a private recording medium wherein the called party can later retrieve the messages.

### **General Principles**

It is generally recognized that most electronic communications are temporary in nature and can be routinely discarded. However, on occasion these communications may also take on the properties of a record, thereby requiring active management under the County's records retention by-law. For the purposes of this policy, a record can be defined as recorded communications made or received in connection with official County business that are retained because they contain evidence which has a direct bearing upon the outcome of that business. The overlying principle in this policy is that decisions regarding retention of electronic communications and the extent to which they constitute a corporate record are at the discretion of the end-user. The end-user must assess if the communication's content affects the County's corporate interests and must decide if on-going retention is required to protect those interests.

---

A further principle of this policy is that electronic communications are not a record series of their own. Retention is determined by the content of the communication, not the format. For instance, an electronic communication pertaining to the outcome of a tender application should be retained and filed in the appropriate file folder for tender applications along with other records if the end-user determines that the communication has a binding impact on the outcome of the tender and if it could impact the corporation's interests in that tender.

### **Methods of Retention**

Electronic communications, particularly electronic mail systems, are not storage mechanisms on their own. Back-up tapes produced by Information Technology are for disaster recovery purpose only and should not be viewed as a method of retention. "In-boxes" and "sent messages" folders are also not formal methods of retention and may be subject to culling upon notice by the Director of Information Technology. To ensure an electronic communication is retained, it must be filed. The following procedures are recommended for those electronic communications that require on-going retention:

1. For electronic mail, users are encouraged to create a permanent file folder within Outlook in which both sent messages and any in-bound messages of corporate interest can be filed. One simple approach is to establish a permanent folder each year within the "Cabinet" section of Outlook. This folder could be called "Permanent2006". It is recommended that a new file folder be created each year for future retrieval and retention review purposes. Alternatively, users can also establish a permanent folder within "Cabinet" that corresponds to a specific file code under the County's records retention policy. This should also be established on an annual basis. Using the example of tender applications, all messages pertaining to this subject which need to be retained can be filed in a folder called "F18-2006".

- 
2. Electronic mail messages can be transferred to Laserfiche (the County's electronic document management system) using the software's "snapshot" feature. The message can then be added to the appropriate electronic folder along with all other relevant documentation. This approach has the added benefit of immediately linking the content of messages with all other types of documentation in a manner that is much easier to search and that still has legal standing as evidence. The original message in Outlook can then be deleted given that Laserfiche preserves the "meta-data" behind that message for legal admissibility. Further guidance on how to use this feature can be obtained from the County's Information Technology Department.
  3. Electronic communications can be printed and filed in the appropriate paper-based folder. In such cases, the electronic communication should also be maintained using one of the above methods in order to preserve meta-data for legal reasons.

It is also possible to convert important voice mails and text messages into a permanent folder within Outlook and ultimately Laserfiche. Staff within Information Technology can provide further guidance on how to utilize this feature.

### **Responsibility for Retention**

The sender of the electronic communication is responsible for ensuring proper retention of messages sent intra-County. All other copies are duplicates and may be deleted. Communications from outside of the County are the responsibility of the recipient. Previous responses to the same message should be deleted as further communications take place. Users should avoid retaining each stage of a forwarded message or response. Only the latest communication should be retained as long as it contains the message history.

County of Elgin

Section: **13**

Human Resources Policy Manual

Subject: **Acceptable Use Policy  
For Computer Equipment,  
Software, Internet Access  
and Internet E-mail**

Code - **A**

Policy Number: **13.10**

Date Approved: **July 24/01**

Page 10 of 10

Date Last Revision: **Feb 12/08**

### **Electronic Mail Attachments**

Attachments should be retained or disposed of according to the content of the attachment itself, not the e-mail which transmits the attachment. Thus, attachments should be retained if they constitute a document which the recipient or the sender would ordinarily retain in the course of the County's business under the County's records retention policy.

### **Electronic Communications as County Property**

Electronic communications sent or received on County equipment are the property of the County of Elgin and may be subject to inspection and review under the County's "Acceptable Use Policy for Computer Equipment, Software, Internet Access and Internet E-mail". This policy applies to the communications of current and former employees.



## EMPLOYEE ACKNOWLEDGEMENT

I have received, read and understood the preceding Acceptable use Policy for Computer Equipment, Software, Internet Access and Internet E-mail for the Corporation of the County of Elgin (Human Resources Policy 13.10).

\_\_\_\_\_  
Employee Name (please print)

\_\_\_\_\_  
Department (please print)

\_\_\_\_\_  
Signature of Employee

\_\_\_\_\_  
Date