Council Policy

Council Policy No.:	C 134 CAO 026
Council Policy Name:	Confidentiality of Information Policy
Date Approved by Council:	May 9, 2006 CR2006-437
Date revision approved by Council:	

Policy Statement and Rationale:

It is important for the Corporation to set out a policy to protect the confidentiality of corporate records of the City of Kawartha Lakes. It is acknowledged that Members of Council, ~~and~~ Committees, Task Forces ~~and~~ staff have access to corporate records which are confidential in nature. It is also acknowledged that these individuals do not complete all City work in a conventional office space within City owned facilities and that City documents may have to be taken off-site to allow work in other locations such as home, meetings, or other public places.

~~This policy is developed in conjunction with the Information Technology Security Policy~~.

Scope:

This policy applies to any person conducting City business ~~using technology provided by the City of Kawartha Lakes~~ and applies to all Members of Council, ~~and~~ all employees and appointed volunteers hereinafter referred to as "system user". ~~Where this policy conflicts with Policy Number 090 ADM 004 – Council Computer Policy 2004, Policy Number 090 ADM 004 – Council Computer Policy 2004 shall prevail.~~

Definitions:

~~Refer to Policy Number 131 CAO 023, Definitions for Policies relating to Electronic Records and Information Technology Assets for definitions relating to this policy.~~

~~Other Related Policies~~

This policy should be read in conjunction with all applicable Corporate Policies and Management Directives~~the following policies:~~

- ~~Definitions for Policies relating to Electronic Records and Information Technology Assets~~

- ~~Electronic Mail Protocol~~
- ~~Electronic Records Management Program~~
- ~~Information Technology Security~~

~~Records Management and Electronic Service Delivery – Privacy Standard~~

- ~~Appropriate Use of Email~~Email
- ~~Appropriate Use of Internet~~
- ~~Appropriate Use of Software~~
- ~~Management of E-mail~~Email

Policy, Procedure and Implementation:

1. MFIPPA, ~~PIPEDA,~~ PHIPA, PIPEDA ~~and~~ QCIPA

1.1 The City of Kawartha Lakes, its Council, staff and appointed volunteers shall comply with the MFIPPA, PHIPA, PIPEDA and QCIPA.

2. Sale or Release of Information

2.1 The City of Kawartha Lakes will not sell personal and/or confidential information.

2.2 The City of Kawartha Lakes will not release personal and/or confidential information unless required by or otherwise in accordance with law and relevant City Policy.

3. Collection of Information

3.1 The collection of information by the City will be governed by legislation, the Records Retention By-law and adopted City ~~p~~Policies.

4. Disclaimer

4.1 The following disclaimer shall be placed at the bottom of all ~~on all~~ emails and fax cover letters ~~es and automatically on all~~ E-mail~~emails b~~being sent externally:

> **This message, including any attachments, is privileged and intended only for the addressee(s) named above. If you are not the intended recipient, you must not read, use or disseminate the information**

contained in this ~~E-mail~~email/fax. If you have received this ~~E-mail~~email/fax transmission in error, please notify the sender immediately by telephone, fax or ~~E-mail~~email and permanently delete this ~~E-mail~~email from your computer/shred this fax, including any attachments, without making a copy. Access to this ~~E-mail~~email/fax by anyone else is unauthorized. Thank you.

4.2 ~~Council, and employees shall place t~~~~The disclaimer noted above shall appear at the bottom of all external E-mail~~email~~.~~

4.3 The City ~~web site~~website shall have a disclaimer relating to any links to other ~~web site~~websites, Access to Information, and Privacy matters . The City shall not be responsible for the privacy practices of such linked ~~web site~~websites.

~~5. Storage of Personal Information~~

~~**5.1 Electronic records containing personal information shall be stored in password protected files, whether the data is stored on a computer hard-drive, network, disk or CD.**~~

~~**5.2 Access to home computers and laptops that contain personal information shall be password protected and controlled. Power-on passwords are to be employed for all desktop, laptop computers and personal digital assistants.**~~

~~**5.3 Council and employees shall not save passwords in physical or electronic form.**~~

~~**5.4 Council members and employees shall lock confidential or personal records in a restricted area, and in a filing cabinet or desk drawer when not being used and/or ensure their office is locked.**~~

6. Personal or other Confidential Information

6.1 If it is necessary to ~~fax or~~ photocopy or electronically transmit personal or other confidential information, Council and employees shall do so directly and/or it shall be delegated to a staff member who is authorized to handle confidential materials and who has signed a confidentiality agreement.

6.2 All members of Council, and employees shall sign a confidentiality agreement as a condition of ~~employment/~~appointment/employment.

6.3 Council and/or employees shall only send personal or other confidential information by ~~E-mail~~email when there is no other option available. The preferred option will be hand delivery. If sending personal or other confidential

information by ~~E-mail~~email, the ~~E-mail~~email shall be classified as confidential using the ~~"Option" features~~ confidential sensitivity tag. For internal ~~E-mail~~email, the wor~~dk~~d **Confidential** shall be placed on the subject line in addition to the confidential classification.

6.4 Confidential information shall be prominently labeled **Confidential** on each page. (Example by using a watermark or the header option).

6.5 Only ~~O~~orange ~~or Purple Paper~~ (salmon) coloured paper is to be used for copies of confidential documents. Members of Council and Senior Staff who receive confidential information on orange ~~or purple~~ paper shall provide the copies to the ~~Clerk~~City Clerk at the end of the Council session where the matter was dealt with unless they are responsible for following through on a matter of action, and the Clerk shall ensure that the information is shredded.

6.6 When bulk physical records (i.e. paper copies or an electronic memory device) containing confidential or personal information (i.e. reporting to a third party, relating to vital statistics, or financial reporting) are to be delivered externally, staff or Council shall use a traceable courier to protect the integrity of the delivery. Letters being sent directly to individual residents are permitted to be mailed by regular post, unless registered mail is required. ~~Personal or other Confidential Information in print form and forming corporate records shall be disposed of by shredding and not recycling in accordance with the Records Retention By-law. Copies of personal or other confidential information shall be disposed of by shredding and not recycling.~~

7. Off-~~s~~Site W~~w~~ork on Files C~~c~~ontaining Personal Information

7.1 Records containing personal information shall only be removed from the office if it is absolutely necessary to carry out work responsibilities. When possible, original documents shall remain in the office and only copies of information shall be removed. Employees shall notify other departmental staff (preferably a supervisor or manager) when removing records containing personal information from the office.

7.2 Paper records containing personal or confidential information shall be kept ~~covered in file folders and contained in a locked briefcase or sealed box~~in a secure location and~~,~~ under the ~~the member of Council or employee~~ constant control the member of Council or employee.

7.3 Work-related records shall be kept separately in only one location of a personal premises.

7.4 ~~Disks or CD's~~ Memory d~~D~~evices containing personal information shall be kept under constant control while in transit and when working away from the office.

8. Loss or Theft

It is the responsibility of every member of Council, staff or volunteer to complete the actions outlined in this section to ensure protection of corporate records.

8.1 Any breach of security shall be reported to the employees immediate supervisor. In the case of Members of Council, breaches of security should be reported to the ~~Mayor and/or the CAO~~City Clerk or their delegate.

8.2 In the event of a lost or stolen laptop, mobile phone, or memory device containing personal and confidential information, it should be reported immediately to the IT Division as well as the ~~Mayor (in case of a member of Council) or the immediate supervisor.~~City Clerk or their delegate.

8.3 If necessary, the ~~Clerk~~City Clerk will contact ~~the police and~~ the Information and Privacy Commissioner ~~of Information and Privacy~~, and the police (if necessary) ~~a~~and follow all appropriate privacy breach policy and procedures.~~.~~

8.4 ~~If necessary, the Clerk will contact individual(s) whose personal information has been lost or stolen and will work with the member of council/employee/volunteer and their supervisor to contain the loss.~~

8.5 Every member of Council and all employees shall assess control of personal or confidential information and records and improve controls wherever possible, in consultation with the City Clerk's Office.

~~9. Release of Personal Information~~

~~9.1 Any member of council or staff receiving a request for personal information shall only release such information in accordance with the MFIPPA, PHIPA, PIPEDA and QCIPA. If the member of council or staff is unsure if it is appropriate for the release of the information, they shall contact the Deputy Clerk - Legislative Services or Clerk by phone or E-mail to ensure that the information is releasable.~~

~~9.2 Where a written request has been received, that request shall be forwarded to the Clerk's Office.~~

~~9.3 The Deputy Clerk - Legislative Services or Clerk will determine the nature of the request and whether a formal Freedom of Information request and associated fee may be applicable.~~

10. Policy Compliance

10.1 Compliance with this policy is mandatory for all members of Council, and employees.

10.2 The contact person for this policy is the City Clerk or Deputy Clerk. ~~- Legislative Services or Clerk.~~

~~10.3 Duties of the Clerk~~City Clerk ~~and Deputy Clerk – Legislative Services with respect to this policy include the following:~~

- ~~Receive and respond to complaints;~~
- ~~Address requests to correct personal information under the City's control (may require statements of disagreement to be attached to the record);~~
- ~~Act as the key contact in any appeal to the Information and Privacy Commissioner;~~
- ~~Provide training opportunities and share information with members of Council, staff and volunteers;~~
- ~~Maintain an index of the City's personal information banks;~~
- ~~Update policy as required;~~
- ~~Work with legal counsel when required, to determine what is releasable.~~

Revision History:

Proposed Date of Review:

Revision	Date	Description of Changes	Requested By
1	May 9, 2006	Initial Release	