PERSONAL INFORMATION PROTECTION
A.7.1

PURPOSE:
All employees at one time or another may receive personal, privileged and/or confidential information which may concern other employees, company operations or clients/customers. The following procedures are designed to preserve the privacy of employees, clients and South Essex Community Counci..

PROCEDURES

All employees will protect and respect confidential and personal information by:

a) Taking all reasonable steps to secure and protect information as follows:

   i) Electronic records of personal information will be subject to limited access by authorized personnel in the performance of their duties.

   ii) Printed records of personal information, when they are not under the control of authorized personnel, will be kept in a secure location.

b) Disclosing to individuals that personal information is being collected and directing them to the SECC Privacy Policy.

c) Destroying the information when it is no longer required, as per funder guidelines.

Privacy Officer

The Executive Director, or his/her designate, will act as the Privacy Officer for South Essex Community Council and will be publicly available as the point of contact for all inquiries or issues related to privacy of personal information.

The Privacy Officer is responsible for:

a) Development and maintenance of the organization's privacy policies both for the public record and for employee records.

b) Thorough review of the organization's collection, use and disclosure of personal information to ensure that only required information is dealt with.

c) Communication of the Privacy policy for the public to the public and to all employees, including necessary employee training.

d) Communication of the Privacy Policy for employee information to all employees, including necessary management training.

e) Acting as an expert resource for the organization on matters relating to privacy of personal information.

f) Ensuring that the organization's systems and procedures meet all legal compliance requirements and also a standard of excellence for respect of personal information.

g) Documenting and analyzing all complaints regarding the use, retention or disclosure of personal information.

h) Instituting changes to the policy and related procedures he or she deems necessary in order to respect the principles of this policy.

i) Notifying appropriate and affected parties of any breach of privacy within 24 hours of being made aware of any such breach.

Guidelines

a) Personal information may be collected without knowledge or consent only in the following circumstances:

- In the event of an emergency that threatens the life, health or security of an individual
- If there are reasonable grounds to believe that the information could be useful to investigate the contravention of a law
- The collection is in the interest of the individual and consent cannot be obtained in a timely way
- The collection of the information with the individual's knowledge or consent would compromise the availability of accuracy of the information and the collection is required to investigate the contravention of a law
- The information is publicly available

b) Personal information may be disclosed without knowledge or consent only in the following circumstances:

- In the event of an emergency that threatens the life, health or security of an individual

- To a lawyer representing the organization
- To collect a debt owed to the organization by the individual
- To a government institution that has indicated disclosure is required on a matter relating to national security or the conduct of international affairs
- The information is publicly available
- If required by law
- For other circumstances listed in subsection 7 (3) of PIPEDA

c) Requests from an individual to provide information about their personal information being collected, use or disclosed by the organization will be answered within 20 days. No fee will be charged for this service.

d) Procedures for Employee requests to access personnel files are outlined in Article 11.04 in the Collective Agreement.

e) If an individual withdraws consent for the use of personal information, the Privacy Officer will take all necessary steps to cease the organization's use of the information within 30 days.