NEW CANADIANS CENTRE PETERBOROUGH

221 Romaine Street
Peterborough, ON K9J 2C3

Tel (705) 743.0882
Fax (705) 743.6219

info@nccpeterborough.ca
www.nccpeterborough.ca

NEW CANADIANS CENTRE PETERBOROUGH

Policy Name: Confidentiality Policy	**Effective Date: Approved April 30, 2008**
Policy Type: Operations / Governance	**Review Date: May 2013**

New Canadians Centre Peterborough is committed to providing confidential services to clients and fostering an environment where personal information is protected. The Executive Director is responsible for protecting confidentiality and ensuring that this policy is carried out effectively.

1.0 Client Confidentiality

1.1 The agency undertakes to keep client records and provide services in as confidential a manner as possible. All clients shall be informed of the agency's approach to confidentiality.

1.2 Only personal information that is reasonably necessary to provide services shall be collected from clients. Staff (and where applicable, volunteers) shall explain to clients why information is being collected and for what purposes the information will be used.

1.3 If information that is reasonably necessary includes documents, staff may make copies with the consent of the client. Original documents shall normally be returned to the client immediately.

1.4 The personal information of a client will only be disclosed to a third party on a need to know basis where the client has given informed consent to the disclosure or where otherwise required by law or where the result of withholding information could reasonably result in serious harm.

1.5 In non-serious harm situations, staff shall obtain written consent from a client (usually via a client consent form) before releasing detailed or important personal information to a third party.

1.6 Clients shall meet with the staff member(s)/volunteer(s) assisting them in private space. Another staff member who shares workspace may be present if not meeting with other clients. Staff members who share workspace shall not meet with clients on separate matters at the same time.

1.7 Communication with clients shall be made in a confidential manner. Particular care shall be taken when leaving voicemail messages and sending email messages.

2.0 Publicity

2.1 The personal information of clients shall not be communicated to media or others for publicity purposes except with the express informed consent of the client. The agency may communicate statistical information without identifying details.

3.0 Files & Staff Access

3.1 Client files shall be accessed only by staff and volunteers who have signed a confidentiality oath and who reasonably require access to the information in order to provide services and collect/tabulate data. Professional auditors may also access information to the extent required by law.

3.2 The personal information of each client shall be kept in distinct paper and electronic files that are clearly labeled and housed in an organized manner. The opening of a new client file shall be recorded in a master database.

3.3 There shall be one central paper file for each client which may be comprised of subfiles. All of the information for a client shall be kept together in the central file where feasible. Subfiles housed separately (e.g. employment files) shall be added to the central file when they are no longer active. A prominent note shall be made in the central file where there is a separately-housed subfile(s), such note including the subfile type, date opened and location where housed.

3.4 Paper files shall be housed in locked cabinets when not in use and shall not be left unattended in public areas of the agency. Cabinet keys shall be kept securely and access limited to staff members who have signed a confidentiality oath.

3.5 Paper files shall not be removed from agency premises unless authorization is provided by the Executive Director. Files taken off agency premises must be kept secure at all times. Volunteers are not permitted to take files off agency premises.

3.6 Electronic files shall be password protected and saved in a central location on the shared drive. Additional up-to-date technological precautions shall be taken to ensure that files are maintained securely (e.g. firewalls, anti-spyware, virus protection). Passwords shall be changed at least twice a year. Staff shall avoid using non-agency computers and personal email accounts to transmit client information.

3.7 Client files are the property of the agency. Closed files shall be destroyed after a period of seven years of inactivity. A record of destroyed files including client contact information and what services were provided shall be kept indefinitely.

3.8 All documentation containing personal information to be destroyed shall be shredded.

4.0 Client Access

4.1 Clients may request to access their file. The file shall be made available for viewing by the client within a reasonable amount of time following a request. The viewing shall be overseen by a staff member. Personal information about other people shall be excised from the file material before it is made available for viewing. The agency may hold back staff notes and observations at the agency's discretion.

4.2 Clients may request a copy of their agency file. The agency may charge the client a reasonable fee to copy a file based on the agency's general photocopy rate plus staff time if significant. The agency shall provide the client a quote in advance if copying costs will be over $10.00 and may provide a quote in any case.

5.0 Staff Confidentiality

5.1 All staff members are required to sign an oath of confidentiality. A copy of this policy shall be given to each staff member.

5.2 The obligation to maintain client confidentiality continues indefinitely.

5.3 Staff members shall not discuss personal client information in public areas (inside or outside of the agency) or in the presence of anyone not bound by a confidentiality oath. Any discussion shall be in the furtherance of service-delivery.

5.4 The personal information of staff members will also be kept in as confidential manner as possible by the Executive Director as governed by the Personnel Policy.

6.0 Volunteer Confidentiality

6.1 Volunteer access to client personal information shall be restricted to volunteers who have been authorized by the Executive Director to deliver services, have a need to know, have signed a confidentiality oath and have reviewed a copy of this policy.

6.2 The Executive Director shall assign a staff member to each volunteer who is granted access to client personal information. The staff member shall supervise the activities of the volunteer and work to ensure that confidentiality is protected.

6.3 Volunteers are otherwise bound by the same confidentiality principles as govern staff members.

6.4 The personal information of volunteers shall be kept in as confidential manner as possible by the Executive Director and Volunteer Coordinator. The names of volunteers are not confidential.

7.0 Privacy of Members and Individual Donors

7.1 The agency shall keep the personal contact information and records of individual donors and members confidential. The agency shall not sell to or trade with third parties the personal information of members or donors.

7.2 The names of members are not confidential.

7.3 The agency will canvass with donors whether or not a donation is made confidentially. Usually the name of a donor will only be kept confidential if the donor has requested anonymity.

8.0 Building Best Practices

The agency undertakes to build best practices around confidentiality. The first draft of a best practices guideline is appended to this policy. Staff will continue to develop the guideline as this policy is put into practice.

Do you have feedback about this policy? NCCP endeavors to review the agency's policies regularly. Please contact the Executive Director with any comments and suggestions to forward to the Policy Committee of the Board.

CONFIDENTIALITY BEST PRACTICES

Last updated October 2007

This document is intended to be developed further as the Confidentiality Policy is put into practice. Contact Ziysah with feedback, suggestions, etc.

Governing Principles

The following principles shall govern the collection and use of client personal information. Information should be:

- **adequate, relevant & not excessive**
- **accurate and up-to-date**
- **accessed only by those who need to know**
- **not kept longer than necessary**
- **kept securely**
- **disposed of carefully**

A. Access / Master listing of files

1. The central filing system poses a challenge to the "need to know" principle. Full access to client files should be restricted to staff members and volunteers who legitimately need to know. If a volunteer is assisting to deliver services, they do not necessarily require access to the whole or even part of the client file. It may suffice for a staff member to give the volunteer a briefing about the applicable background information.

2. The policy requires at 3.2 that the opening of new client files be recorded in a master database. Recent practice has been to do so in the "newcomer's list" although that list wasn't designed to facilitate access to files or to ensure that files do not go missing. The OCASI database is currently in development and is set to be available in 2009. Using the "newcomer's list" will probably suffice until then although staff are encouraged to think of interim improvements to track files in a more organized way (e.g. allocate numbers to files).

B. Consent

1. The policy requires that staff obtain written consent in order to release detailed or important client personal information to a third party. Staff should err on the side of caution and obtain written consent even if it is not clearly required.

2. Consent that is given verbally by a client should be noted in the client's file. The note will include the details of the authorization, and the date, time and name of the staff or volunteer who received the authorization.

3. It may be appropriate to confirm that consent was given in a letter or email to the client.

C. Communication

1. Clients should be asked about what mode of communication is best for them and what confidentiality concerns there may be with different forms of communication. A section will be added to the intake form so that these questions are standardized and to ensure that responses are recorded. Careful judgment should be exercised by staff/volunteers regarding the best way to communicate with particular clients and related notes may be made in the file (e.g. "Do not call at home after 3:00 pm").

2. Voicemail messages left by staff/volunteers for clients should not contain confidential details if the mailbox can be accessed by other people. In some instances a voicemail should not even include the name of the agency. A brief call-back request message can be left using a first name (example below). If a client's situation is particularly sensitive, it may be advisable not to leave a message at all. Notes should be kept of voicemails left.

> "This is a message for [first name] from [first name]. I am calling Monday at 2:00 pm. Would you please call me back at 743.0882. Thank you."

3. The agency's phone number may be blocked free of charge using the *67 feature (see telephone book). This feature should be used in sensitive situations.

4. Particular care should also be taken with conveying personal information by email. Email can be sent to the wrong address with the click of a button. Addresses should be double checked and before relaying personal information, staff should ensure that only the client has access to the account. Copies of emails should be printed for the paper file.

5. Email should only be sent to clients from official agency addresses (never the personal accounts of staff or volunteers). Each account should be set up with a confidentiality disclaimer that is added automatically to each communication:

> This communication is intended solely for the addresse(s) and may contain confidential information. If you have received this email in error, please notify the sender immediately by return email and permanently delete all record of the communication. Many thanks.

6. Confidential information should be cleared from email in-boxes on a regular basis and stored in a central electronic and/or paper file.

D. Computers / Electronic files

1. Staff computers should be kept up-to-date with standard protections (firewalls, virus scanners, anti spy-ware) with password protected automatic standby mode installed. Passwords should be changed every six months.

2. The policy requires at 3.6 that electronic files containing client information be saved on the shared drive. Files should be clearly titled and saved to the client's individual folder on the shared drive and not to individual drives (e.g. C drive, 'my documents').

3. Staff shall avoid using personal email accounts and personal computers to transmit or house client information. If it is necessary to do so, the personal information shall be permanently deleted as quickly as possible. Volunteers should never use personal email accounts and personal computers to transmit or house client information.

4. The above principles shall also apply to the personal information of members, donors, staff, volunteers and prospective staff though it is recognized that sometimes volunteers receive personal information about staff/prospective staff and volunteers over email (e.g. board members receive copies of resumes). The delete as soon as possible principle applies.

5. Client information should not be accessed through the public computers due to their public nature.

6. For further consideration: the possible security limitations of remote access and the general security of agency computers against theft.

E. To consider next policy review – Spring 2010

- Consider appointing a staff member as a privacy officer. Role would be to take inventory of personal information, oversee implementation of policy, give advice on confidentiality matters, and educate staff and volunteers.

- How the policy needs to be updated in light of the OCASI client database which is expected to be rolled out in 2009.