YMCA-YWCA Newcomer Services Privacy & Security Guidelines - Pre-Arrival Settlement Services

Developed: May 2017

Last update: May 2017

In order to comply with privacy and security requirements imposed by Immigration, Refugees and Citizenship Canada and to uphold best practices within the YMCA-YWCA of the National Capital Region, the following guidelines must be respected.

Information from IRCC:

- IRCC's "Gathering Information" pamphlet must be posted on the Privacy Policy page on the Build ON website and linked in our registration form
    - Clients must be provided with this pamphlet in their language of choice (available through iCARE) upon request

iCARE access:

- Web browsers accessing iCARE must be updated regularly to ensure that the most recent version available is in use
- iCARE passwords must not be written down nor posted anywhere in your workspace
- iCARE login and password information must be shared with the Director, who will store the information in a protected document in case it is needed for retrieval
    - Director must be informed of updates or changes to your iCARE password
- iCARE login information must not be shared with anyone else; anyone accessing iCARE should have their own individual account
- Requests for new iCARE accounts must go through the Director
- When accessing iCARE through wifi, only secure (password protected) private wifi networks should be used

Collection and disposal of client information:

- Clients must not be asked to provide personal information outside of what is required for entry into iCARE and that which is required to provide the requested service (i.e. information to be input in CATS and the client database as per Build ON admin guidelines)
- Staff providing client service must ask for verification of client information by asking to see a copy of one of the following immigration documents via encrypted video chat or sent through applications with end to end encryption (whenever possible)
    - An IRCC invitation letter to obtain pre-arrival services

    - A Confirmation of Permanent Residence (COPR) letter
    - A passport request letter that indicates Permanent Resident visa issuance
    - An IRCC request that an applicant for permanent residence complete medicals
    - A Single Entry Permanent Resident Visa
    - A Permanent Resident Visa pick up notification letter
- If clients provide staff with copies of their immigration documents, all digital and physical records of these documents must be securely destroyed immediately following visual verification of the client's information
- Client information must be disposed of in the following manner once it is no longer required:
    - Physical records must be shredded
    - Digital records must be placed in the Recycle Bin and the Recycle Bin must be emptied immediately
    - A case note must appear in CATS indicating that client information was securely disposed of, including the date on which it was disposed

Physical security:

- Computers must be password protected (screen locked) any time that staff is not present at their desk
    - All computers must have a screen-saver with password protection with an activation period of no more than 15 minutes of non-usage
    - Passwords must be changed every 3 months
    - Updates to passwords must be communicated to the Director, who will store the information in a protected document in case it is needed for retrieval
- Build ON smart phones are to be kept in a locked drawer in the Build ON office when not in use
- Build ON smart phones are to be passcode protected at all times when not in use
    - Passcodes should be changed every 3 months
    - Updates to passcodes must be communicated to the Director, who will store the information in a protected document in case it is needed for retrieval
- Build ON smart phones are not to act as document repositories containing personal client information

    - Personal client information received via a Build ON smart phone must be transferred to secure digital storage (see below) and permanently deleted from the phone

- Client information must not be stored on portable data storage devices (i.e. memory sticks, external hard drives, etc.)

    - In the event that client information is temporarily stored on a portable data storage device, information must be transferred to secure digital storage and permanently deleted from the portable device as soon as possible

- Staff will determine the appropriate venue for meeting with clients depending upon their needs (i.e. if voice chat is being used, staff should meet clients in a private space outside of public earshot)

- Computer/smart phone screens should not be in public view when working directly with a client and/or when viewing or working with client information

Disclosure and privacy of client information:

- Client information must only be used for data entry in iCARE and internal statistical purposes and must never be shared with external parties without the client's consent

    - Verbal or written consent must be obtained and recorded in case notes for referrals to external partners (including to OCISO for Build ON mentorship) for which client information must be shared

- Individually identifying client information (for example, name + UCI#, UCI# + birth date) should not be shared by e-mail unless encryption is in place

- Client information should be discussed between staff only when necessary and in appropriately private areas (not within public earshot)

- Staff are expected to respect the anonymity of all Y clients in public, including online "public" channels such as on social media

- Clients are entitled access to information that the Y has gathered and stored about them upon request

    - If such a request is made, notify the Director immediately

    - Personal information must be sent to the client through a secure channel, such as via end-to-end encrypted message (i.e. WhatsApp, Viber, etc.)

    - If a secure digital channel is not available, client's personal information may be shared with them via phone call or first-class mail

    - All personal information shared with client must be labelled "Protected B"

- In the event that there is a suspected privacy breach (i.e. a computer containing personal client information goes missing, etc.), the Director must be informed immediately

Storage of client information:

- Client information must only be stored digitally in the following secure locations:
    - Client's individual file on the shared drive
    - Client database on the shared drive
    - CATS
    - iCARE
- Personal client information sent via e-mail must be transferred to a secure digital storage location immediately
    - Non-encrypted e-mails containing personal client information must be deleted as soon as the information has been transferred to a secure location
- Physical records of client information should not be kept in any format
    - In the event that temporary physical records are created (for example, staff writes down notes during a meeting that includes client name, contact information, etc.) the following guidelines must be followed:
        - Information must be kept out of public view while being used
        - Information must be stored in a locked drawer when not in use
        - Information must be securely destroyed (i.e. shredded) as soon as it is no longer needed

Case notes:

- All clients who complete the Build ON registration form must check a box indicating consent for registration, which includes the Build ON privacy policy (otherwise they cannot proceed with registration). A case note in CATS (first client meeting) must indicate that the client has consented to Build ON's privacy policy.
- A note must appear in CATS case notes indicating that client information was verified by seeing a copy of the client's immigration document

    - If staff receive a digital or physical copy of clients' immigration documents, a note must appear in case notes indicating that documents were securely destroyed

- Any request made by a client to access their own information must be documented via case notes in CATS
- In the event that referrals that are made to external organizations which require sharing of client information a note must appear in the client's case notes that they consented to the sharing of their information with that partner
    - Indicate whether consent was written or verbal

Privacy and security awareness statement

I hereby declare that I have read and understand the above guidelines. In signing I agree to respect these guidelines and to communicate with my supervisor should I have any questions or concerns with regards to ensuring the privacy and security of client information. I acknowledge that these guidelines are subject to change and I may be required to sign updated versions of this document throughout my employment with the YMCA-YWCA of the National Capital Region's Newcomer/Employment Services.

Staff name: _____

Staff signature: _____

Director name: _____

Director signature: _____

Date: _____