USE OF TECHNOLOGY

POLICY TEMPLATE GUIDE FOR WOMEN'S SHELTERS AND TRANSITION HOUSES

Tech Safety Canada

ACKNOWLEDGEMENTS

We gratefully acknowledge the BC Society of Transition Houses and the National Network to End Domestic Violence for sharing their work and expertise about the impact of anti-violence organizations' use of technology on women, children and youth's privacy, confidentiality, and safety. The work of both organizations has contributed to the development of this guide.

Tech Safety Canada is a project of Women's Shelters Canada.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada
Femmes et Égalité des genres Canada

TABLE OF CONTENTS

Overview

This guide offers sample policy templates to assist anti-violence organizations to develop specific "use of technology" policies for violence against women (VAW) shelters and transition houses.[1]

These policy templates were created to ensure that the way technology is used in our collective work to support women, children, and youth experiencing domestic violence does not negatively impact the privacy, confidentiality and safety of the people who access our services. The policy templates included in this resource specifically address the use of technology by board members, employees (including the Executive Director), subcontractors, service providers, volunteers, trainees, and work placement and student interns working within VAW shelters and transition houses.

The policy templates included in this guide reflect:

- Funder contractual obligations
- current legislation; and
- use of technology best practice.

The policy templates provided are meant to supplement current organizational, and specific women' shelter and transition house policies. It does not presume to dictate the contents of policy for individual organizations but instead provide a possible framework in which personnel working within a Women's Shelter or Transition Housing Organization can use technology in a way that is attentive to the safety and privacy of women, children, and youth that access their organizations[2].

Not all policies will apply to all VAW shelters and transition houses, so personnel and administrators are encouraged to review these templates and adapt them to their organizational contexts and the technology they use. For example, in this guide, sample policies for fax machines, scanners, and printers are written as if organizations have three separate devices. However, we know that many organizations use "all in one" devices and, therefore, these policies can be combined in a way that makes sense for your organization.

[1] Throughout this document, the language of VAW shelters and transition houses will be used to reflect women's shelters, transition houses, second and third stage shelters/houses, and safe homes for women and children fleeing violence.

[2] For technology safety policies specific to the PEACE Organization, the "PEACE Organization Use of Technology Policy Template Guide" can be found at https://bcsth.ca/publications/Transition House-organization-use-of-technology-policy-template-guide.

The sample policy templates include a variety of headings for clarity. They include:

- Rationale: The rationale represents the "why" of the policy. A statement of justification that details why the policy has been developed and why it is important to the service. The rationale gives context (political and/or organizational) to the policy development. (OAITH, 2010)
- Policy Statement: The policy statement describes the rules, guidelines and boundaries of a specific issue. This statement should demonstrate the organization's position or decision about how the organization will carry out its activities. (OAITH, 2010)
- Procedures: Procedures are the "how", the methods to implementing a policy. They are action oriented. Procedures detail who performs the procedure, what steps are performed, when the steps are performed, and how the procedure is performed.
- Policy Creation Date: Date the policy is created.
- Policy Review Date: Date the policy is up for review.
- Policy Designate / Overseen by: Who is responsible for overseeing the policy, for example, finance person, Executive Director, board, volunteer coordinator etc.

For the purposes of this resource, the policy templates include only the rationale, the policy statement, and procedures. The policy created date, the policy review date, and the policy designate, have been left blank as this will vary between organizations depending on when the policy is implemented.

A Note on Language

Throughout this policy guide, we refer to *service users* and *women, children, and youth* accessing services. These terms are interchangeable.

The language of *VAW shelters and transition houses* will be used to reflect women's shelters, transition houses, second and third stage shelters/houses, and safe homes for women and children fleeing violence.

Personnel refers to board members, employees (including the Executive Director and frontline staff), subcontractors, service providers, volunteers, trainees, and work placement and student interns.

Personal information is defined by the Office of the Privacy Commissioner of Canada as information about an identifiable individual which includes any factual or subjective information about that individual, including, for example:

- Name
- Opinions about the individual
- Birth date
- Income
- Physical description
- Medical history
- Gender
- Religion
- Address
- Political affiliations and beliefs
- Education
- Employment
- Visual images such as photographs, and videotape where individuals may be identified

Section 1: Office Technology

1. Office Phones

Rationale: Organization XYZ[3] is committed to ensuring that all women, children, and youth experiencing domestic violence can communicate with VAW shelter and transition house personnel using the safest and most accessible method of communication. Communicating by a landline phone is one of the safest and easiest methods.

Policy Statement: personnel working in VAW shelters and transition houses will communicate with women, children, and youth in the safest and most accessible method that Organization XYZ can provide based on resources and guidelines outlined by provincial privacy laws and the Office of the Privacy Commissioner of Canada. Steps to maintain the confidentiality, privacy and safety of women, children, and youth will be taken.

1.1 Caller ID

Procedures: Organization XYZ's landline phone system is set up to block the organization's phone number and name from showing on the receiver's caller ID. If personnel are in doubt, they will test the system before making a call to (past, current, or potential) service users.

If personnel are calling a service user from a phone that is not set up to block the outgoing number, personnel will manually dial *67 before dialing the number.

Note: Some receivers will reject calls with blocked numbers. personnel may unblock the organization's blocked number once they have:

- Explained any potential safety risks to the service user, such as a perpetrator monitoring her phone call log, and
- Have consent service user that it is safe to unblock the number when calling her.

As it is possible to unblock blocked numbers, safety planning with residents about communicating via phone is important.

[3] When writing their organizational polices, organizations will insert their own organization name in place of "Organization XYZ."

If personnel have any concerns or doubts, they will get approval from their supervisor before making the unblocked phone call.

Note: Organizations using a cloud-based phone system should include policies about the risks of cloud-based phone services and procedures around communicating when there is no power and/or Internet access.

1.2 Voicemail

Procedures:

a) Password: personnel who have been assigned a voicemail box will reset the password of the voicemail box when beginning their employment at Organization XYZ.

b) Voicemail Greeting: When recording a voicemail greeting, voicemail greetings must ask for the caller to state whether it is safe to call back and leave a message when their call is returned. Voicemail greetings will also state the office hours of personnel and an alternative emergency number.

c) Deleting Messages: After listening to voicemail messages, personnel will immediately delete messages. This will be done consistently unless the message needs to be kept and the reasons are documented by the organization supervisor.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

2. Mobile Phones Owned by the Organization

Rationale: Organization XYZ is committed to having safe and accessible technologies available for personnel to provide shelter and transition housing services. Mobile phones, including smartphones, can make it easier for personnel to do their work while working offsite. Mobile phones can help personnel communicate with fellow employees and service users, check calendars, access files from the organizational server, access email, and update any paperwork or reports.

Though their size and portability can be convenient, there are security and confidentiality risks associated with using mobile phones that require careful

consideration. For example, sometimes having the location settings turned on (under a mobile phone's privacy settings) can be useful, for example, to get directions when accompanying a service user to an appointment. Other times, having the location services turned on can inadvertently disclose the location of personnel and participants, giving away the location of a confidential shelter or a service user's address or school.

Other confidentiality and security risks to service user privacy and organization confidentiality to consider are that mobile phones can:

- Easily be stolen or misplaced
- Breach personal information through contacts, call logs, emails and text messages
- Quickly install spyware
- Have cloud servers easily accessed/intercepted for personal information, photos, and videos
- Inadvertently disclose personal information by linking to other devices
- Potentially enable third parties/developers to access personal information when downloading apps. This is because some free applications may access other data stored on the device, such as contacts or pictures.

As all communication can be considered part of a service user record, not using personal mobile phones will help to protect service users, personnel, and Organization XYZ from subpoenas and breach of confidentiality legal action.

Policy Statement: Organization XYZ allows the use of Organization XYZ-owned mobile phones by personnel while they are working offsite, with limitations. All personnel using organization mobile phones will be made aware of the potential safety and security risks (e.g. downloading of apps, cloud server storage) associated with mobile phones and the corresponding policies.

Using mobile phones that are not owned by Organization XYZ can breach the confidentiality of women, children, and youth accessing the shelter and put their privacy and safety at risk. In accordance with the guidelines provided by the Office of the Privacy Commissioner of Canada and various provincial privacy commissioners, using mobile phones not owned by Organization XYZ to communicate with service users is prohibited.

Note: Organizations allowing the use of personal laptops and mobile phones for shelter and transition housing work must comply with the Office of the Privacy Commissioner and provincial privacy guidelines. This includes making employees

aware of employer's rights to access their devices. Please see the Bring Your Own Device Section on page 60.

2.1 Personnel Accounts

Procedures: When Organization XYZ loans a mobile phone to personnel to use for work purposes, the personnel will work with the Administration Manager and/or IT subcontractor to set up an account and User ID and password for their work mobile phone. This ID will not be used with any other device.

2.2 Security: Passwords

Procedures: When Organization XYZ loans a mobile phone to personnel to use for work purposes, the personnel will set up the phone with a unique and strong password. Each personnel's password will be given to the supervisor, Executive Director, or Administration Manager in a sealed envelope, kept in a locked cabinet and only accessed if necessary.

2.3 Storing Contacts

Procedures: Personnel will not save or store any past or present service user's contact information on Organization XYZ owned mobile phones. Names of Organization XYZ personnel can be stored on the phone's contact list on a first name basis only.

2.4 Voicemail

Procedures:

a) Password: Personnel at Organization XYZ who are using mobile phones that have voicemail capability must reset and change the password of the voicemail box when beginning their employment at the organization or when getting a new mobile phone. A copy of the password will be given to the Administration Manager, supervisor, or Executive Director in a sealed envelope and stored in a locked cabinet only to be accessed if necessary.

b) Voicemail Greeting: Personnel at Organization XYZ will clearly record a voicemail greeting that states their office hours when callers can generally expect to receive a reply to their message (typically within 2-3 business days) and an alternate number to contact in case of

emergency. When recording the voicemail greeting, the voicemail must ask for the caller to state whether it is safe to return their call and leave a voicemail on the number provided.

c) Deleting Messages: After listening to voicemail messages, personnel will immediately delete all messages. This will be done consistently unless the message needs to be kept and the reasons are documented by the organization supervisor.

2.5 Caller ID

Procedures: All Organization XYZ mobile phones will be set up to block or turn off caller ID. If a mobile phone is not set up to block the number or show up as private, personnel will manually dial *67 or #31# before they dial the number of any (past, current, or potential) service user.

Some receivers will reject calls with blocked numbers. VAW shelter and transition house personnel may unblock their blocked number once they have:

- Explained any potential safety risks such, as the perpetrator monitoring her phone call log, and,
- Have consent from the service user resident that it is safe to unblock the number when calling her.

If personnel have any concerns or doubts, they will get approval from their supervisor before making the unblocked phone call.

2.6 Personal Use

Procedures: When Organization XYZ loans a mobile phone to personnel to use for work purposes, Organization XYZ will communicate clearly all policies related to personal use of the organization mobile phone. These include policies related to:

- Storage of personal contact information
- Taking and storing personal photos or videos
- Downloading of apps do not work related
- Connecting to other devices
- Location tracking/GPS enabling functions
- Sending and receiving of personal communications

2.7 Ownership and Privacy

Procedures: By law, Organization XYZ must ensure personnel are following the policies about storing and destroying personal information in compliance with your province or territory's privacy laws. If necessary, personnel may be asked to provide their organization-owned mobile phone to review security updates and confirm that deletion of communications are up to date.

In some provinces and territories, personal information in an organization's control may be subject to reasonable and acceptable corporate monitoring.

2.8 Sharing Location and Content

Procedures: Personnel will ensure that location services are turned off on their organization mobile phone when it is not in use.

Personnel will also disable Bluetooth capabilities on their organization mobile phone to minimize the risk of interception (unless needed).

Note: If the location settings are turned on and personnel take a photo or video, the location, date, and time of where the photo/video was taken will be stored on the photo/video metadata (data of the photo).

2.9 Taking Photos and Videos

Procedures: Personnel will only take work-related photos and videos on their Organization XYZ owned mobile phones. u, personnel will inform service users of any risks associated with having their photo or video taken such as posting photos online and storing photos and videos in a cloud server. Storing photos or videos on a cloud server can make it easy for individuals to access and/or intercept personal images.

Personnel will obtain written consent from service users before taking any photos or videos by providing them with a photo consent form. Participants will be informed that they have the right to withdraw their consent to use their image at any time.

2.10 Storing Photos and Videos

Procedures: When setting up Organization XYZ's mobile phones and the accounts associated with them, the Administration Manager and IT

subcontractor will ensure that photos and videos are not backed up to any cloud servers including iCloud or Google Drive. Photos and videos will be deleted within three business days when they are no longer useful or once they have been uploaded to Organization XYZ's main computer network.

2.11 Cloud Backup

Procedures: When setting up Organization XYZ's mobile phones and the accounts associated with them, the Administration Manager and/or IT subcontractor will ensure that the phone's content, including texts, emails, contacts, photos, and videos are not backed up to any cloud servers including iCloud or Google Drive. Personnel will not change these settings to protect their privacy and confidentiality of service users.

2.12 Connecting to Wi-Fi

Procedures: If personnel are working on files and documents that contain any personal information or sensitive details, personnel will not connect to or use public Wi-Fi networks. This includes, but is not limited to, free Wi-Fi networks available in coffee shops, restaurants, airports, community centers, hotels, and libraries. These typically insecure networks are vulnerable to hacking or interception.

2.13 Link to Other Devices

Procedures: Personnel will ensure that the organization-owned mobile phone is not linked to any other devices, possibly through cloud IDs or work-related or personal devices (e.g. iPhones, iPads, MacBooks, and Apple watches). This will make the mobile phone more secure and prevent inadvertent disclosure of any personal information.

2.14 Updating the Mobile Phone

Procedures: One easy security precaution is to keep the mobile phone operating system up to date with the latest operating system versions. personnel will download all available updates to their devices within 5 business days of the newest update available.

2.15 Download of Applications

Procedures: Some applications (apps) give developers access to the phone, including access to an individual's personal information, contacts, and photos. Personnel must be cautious of the types of apps that are downloaded onto organization phones and fully read the Terms and Conditions of each app that they download. personnel will only download apps that are necessary for their work.

If participant information is stored in email, contacts or other areas in the device, it may be possible for the information to be accessed by these apps. personnel will pay close attention to what data these apps are accessing and collecting by reading the permissions, either on the device or the apps website before downloading them to their work mobile.

If personnel have any doubt, they will check with the supervisor, Administration Manager and/or IT subcontractor before downloading an app.

2.16 Deletion of Call Logs, Messages, and Voicemails

Procedures: In compliance with our province or territory's privacy laws, personnel at Organization XYZ will delete the mobile phone's call log, text message log, text messages, and voicemails daily, unless it is necessary to keep. Keeping a text message, photo, email, or voicemail from a (past, current or potential) service user should only be done with permission from a supervisor and/or in some cases the Executive Director. This is because the phone could be monitored and communication intercepted. Furthermore, all communication stored on a mobile phone can be considered part of the service user's record and be subpoenaed.

2.17 Remotely Wiping or Disabling a Phone

Procedures: A copy of the mobile phone account information and passwords will be left onsite with the Administration Manager, Supervisor, or Executive Director in case the Organization XYZ-owned phone is stolen or misplaced. If the phone is stolen or misplaced, personnel will report this to their supervisor immediately. The supervisor will contact the Administration Manager who will then connect with the IT subcontractor to assist in remotely disabling (locking the phone from further use) or wiping (erasing the phone's contents) the phone in case any personally identifying information of service users is on the phone.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

3. Fax Machine

Rationale: Organization XYZ is committed to protecting the privacy and confidentiality of all service users. Personnel must abide by *(insert local privacy law)* or the Personal Information and Electronic Documents Act (PIPEDA) when sending personal information through fax. Faxes are most often used to send documents and referrals on behalf of women, children, and youth accessing support services. Typically, these types of documents contain personal information. If intercepted, accessed or sent to the wrong address, a fax could put service users' privacy and safety at risk.

Most of the fax machines that organizations use have the capacity to store information such as date and fax number of faxes sent and received. Larger machines can store a digital copy of all of the information contained in faxes sent and received. If the fax machine hard drive is not destroyed or the data permanently deleted before returning the machine to the lease company, or donating or recycling, there is a potential for a data breach.

Policy Statement: In compliance with PIPEDA or local privacy acts, personnel will not include personally identifiable information of service users to internal and external organizations via fax without the signed informed consent of the service user that has been documented in the organization's *Release of Information* (ROI) form.[4] Before asking a service user to sign the ROI, personnel will inform the service user of all risks associated with sending a fax containing personal information and their right to revoke consent.

Personnel will follow the recommendations for the faxing of personal information by the Office of the Privacy Commissioner of Canada.

Note: Other policies related to a multifunctional device such as a printer and/or a scanner may also need to be considered.

[4] Sample forms such as Release of Information and Informed Consent forms can be found online in the BCSTH Legal Toolkit https://bcsth.ca/projects/legal-education-resources.

3.1 Sending of Personal Information

Procedures: Before agreeing to send a fax containing a service user's personal information, personnel will inform the service user of any potential risks that could impact her confidentiality, safety, and privacy. This can include, but is not limited to, interception, more than one person at the receiving end having access to her private information and/or her location being compromised by Organization XYZ's fax number and header appearing on the received copy of the fax.

According to some provincial privacy laws, service users must consent to having their information sent via fax. An *Informed Consent* form and Organization XYZ's *Release of Information* form must be provided to service users to complete and sign before faxing. Service users will be informed that they can revoke their Release of Information at any time. This can be done via the organization's *Revocation of Information* form.

All completed *Informed Consent, Release of Information* and *Revocation of Information* forms will be filed in the participant's record.

If there is a privacy or safety concern, personnel will call the receiver of the fax to make sure that the person the fax is intended for is there to pick up the fax and confirm that they have received the document.

Note: Other policies related to a multifunctional device such as a printer and/or a scanner may also need to be considered.

3.2 Receiving Personally Identifying Information

Procedures: Personnel at Organization XYZ will not require service users to send personal information, other than their name and contact number, via fax (such as in *Referral* forms) to access services.

When a service user is expecting personnel to receive a fax containing personal information on their behalf, personnel will ensure that the document is picked up immediately and given to the participant. If the participant is not on site at the time, personnel will store the document in a locked cabinet on site.

3.3 Storage, Purging, and Destruction

Procedures: The Administration Manager in conversation with the Executive Director and Information Technology (IT) subcontractor are responsible for ensuring that all records and memory on the fax machine hard drive is destroyed before the machine is sold, donated, or returned to the leasing company.

Note: Other policies related to a multifunctional device such as a printer and/or a scanner may also need to be considered.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

4. Printer

Rationale: Printers are used to print documents that sometimes contain the personal information of women, children, and youth accessing VAW women's shelters and transition houses. Most printers have an internal hard drive that stores a digital copy of every item printed. If the printer hard drive is not destroyed or contents permanently deleted before it is returned to the lease vendor, donated, or recycled, the personal information of service users could be breached. personnel are committed to ensuring the privacy and safety of women, children, and youth accessing their organizations.

Policy Statement: Personnel at Organization XYZ will comply with privacy legislation when collecting, storing, using, and disclosing the personal information of women, children, and youth accessing VAW shelters and transition houses.

Note: Other policies related to a multifunctional device such as fax machine and/or a scanner may also need to be considered.

4.1 Storage, Purging and Destruction

Procedures: The Administration Manager in conversation with the Executive Director and IT subcontractor is responsible for ensuring that all records and memory from all printers at Organization XYZ are destroyed before the machine is sold, donated, or returned to the leasing company.

Policy Creation Date:
Policy Review Date:

Policy Designate / Overseen by:

5. Scanner

Rationale: Organization XYZ is committed to protecting the privacy and confidentiality of all residents and service users. Most scanners can store a digital copy of the image scanned to the hard drive of the device. Scanners are most often used to make electronic or digital copies of hard copy documents. Typically, these types of documents can contain personal information. If intercepted, the document could put women, children and youth's privacy and safety at risk. personnel must abide by (name of privacy legislation) when copying personal information through a scanner.

Note: Other policies related to a multifunctional device such as a printer and/or a fax machine may also need to be considered.

Policy Statement: In compliance with (name of privacy legislation), personnel at Organization XYZ will ensure the confidentiality, privacy, and safety of women, children, and youth when making copies of documents containing personal information.

5.1 Scanning of Personal Information

Procedures: Before agreeing to scan a document containing a service user's personal information, personnel will inform her of any potential risks that could impact her safety and privacy. This can include, but is not limited to, interception and information being accessed by other Organization XYZ personnel, leasing companies or future owners of the machine.

According to some privacy laws such as BC's PIPA, service users must consent to having their information collected. *Informed Consent* forms and the organization's *Release of Information* form will be given to the participant. If they consent to the release of their information they will complete and sign the forms. Service users will be informed that they can revoke the Release of Information at any time via the Transition House organization's *Revocation of Information* form.

All *Informed Consent, Release of Information* and *Revocation of Information* forms will be filed in the service user's file.

5.2 Storage

Procedures: Service users asking personnel to scan documents on their behalf must be made aware of the possibility that the scanner may store digital copies of their information and any associated potential future risks.

The Administration Manager, IT subcontractor, and Executive Director will research each machine and their storage capacity and set up a plan to routinely delete the hard drive's memory and destroy any documents stored on the machine based on each machine's capabilities.

Service users will be made aware that copies of scanned documents can automatically be downloaded and stored on Organization XYZ's computer network. If the organization's scanner is set up to automatically download copies of documents to the network, print a copy for the participant and delete the electronic copy immediately to prevent inadvertent disclosure of personal information and any security, privacy, and safety risks.

5.3 Purging of Personal Information

Procedures: Organization XYZ's computer network is accessible by staff and third-party vendors and subcontractors. In compliance with (name of local privacy act), no documents containing personally identifying information will be kept on Organization XYZ's computer network. After scanning the document and giving a copy to the service user, personnel will immediately delete all the documents containing personal information from Organization XYZ's network.

5.4 Destruction of Hardware

Procedures: The Administration Manager in conversation with the Executive Director and IT subcontractor will ensure that all copies of documents stored on Organization XYZ's computer network and scanners are destroyed before the machine is sold, donated, or returned to the leasing company.

Note: Other policies related to a multifunctional device such as a printer and/or a fax machine may also need to be considered.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

6. Desktop Computers Owned by Organization

Rationale: Organization XYZ is committed to ensuring that all women, children, and youth experiencing violence can communicate with personnel using the most accessible method of communication for them, and that personnel have the necessary tools to provide services.

Computers have become essential for service delivery. Providing access to computers has also become necessary for service users to be empowered, for example to research schools, connect with family and friends, fill out forms, apply for work, and communicate with supports organizations.

Policy Statement: Organization XYZ provides computers for personnel and for service user use. Service users will access devices, use logins, and Wi-Fi connections that are separate from personnel.

6.1 Passwords

Procedures:

a) Personnel: Supervisors will liaise with the Administration Manager to ensure that all personnel will have a unique User ID login and password to access organization owned computers. A copy of the login and passwords will be given to the supervisor, Administration Manager, or Executive Director and stored in a lock cabinet. When not using the computer, personnel will log off.

b) Service users: The Administration Manager will work with the IT subcontractor to ensure participant-designated computers have a Guest login and password for women, children, and youth wishing to use participant-designated computers. Ideally, service users will use a separate computer from personnel that is participant designated. However, if there is not a computer for participants accessing the shelter or transition house, and the participant must use a computer designated for personnel, personnel will log off and the participant will log in using the Guest login and password provided. This will help to ensure the security of Organization XYZ's computer network and confidentiality and privacy of other participants.

6.2 Security Software

Procedures: The Administration Manager at Organization XYZ will ensure that the IT subcontractor will install anti-virus, anti-spyware software, and anti-malware software on all computers and set up a schedule to ensure that they are routinely updated.

If personnel notice something suspicious or receive a virus warning or alert on their computer or on a computer designated for participants, personnel and service users will discontinue using the computer and report a potential breach to their supervisor or Administration Manager immediately.

6.3 Computer for Service user Use

Procedures: The Administration Manager at Organization XYZ, in partnership with the IT subcontractor, will ensure that guest accounts will be set up without administrator rights. This will make it more difficult for anyone to download anything onto the computer without administrator permission. The Executive Director and IT subcontractor will also ensure that computers designated for service users are not connected to the organization's computer network and will consider disabling file sharing and the ability to remote access into these computers.

Service users are encouraged to use their own USB drives to store documents rather than saving them on organization computers that are accessible to all participants. If women, children, and youth do not have their own USB drive, and when funding permits, USB drives may be available for service users to download and save important documents on. personnel will also discuss the importance of password protecting USB drives with service users.

6.4 Webcam

Procedures: Webcams on computers typically have a visible light that turns on so that the user knows the webcam is on. However, it is possible on some computers to disable the light from turning on. Personnel at Organization XYZ and service users will turn off the webcam when not in use. All Organization XYZ's computers will have a cover on their webcam (e.g. removable sticker, post-it note, tape) when not in use. Webcams will be positioned so that the location of the computer does not inadvertently

reveal any potentially identifying and confidential information such as the location of the organization or reveal the identity of service users.

The Administration Manager, in conjunction with the IT subcontractor and Executive Director, will ensure that anti-virus, anti-spyware, and anti-malware systems are set up to scan Organization XYZ's computers regularly.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

7. Laptops Owned by the Organization

Rationale: Organization XYZ is committed to having safe and accessible technologies available for personnel to provide shelter organization services. Laptops can make it easier for personnel to do their work while working offsite. Laptops can help personnel to access files from the office, access email and update any paperwork or reports.

Though their size and portability can be convenient, there are security and safety risks associated with laptops used for shelter support work. Unlike a desktop computer that is set up in a specific location, laptops can be easily stolen or misplaced. It is also very easy for others to pick up a laptop and scroll through the information, which can include the personal information of women, children, and youth accessing shelter organization services. Someone with malicious intent and with access to a spyware organization could quickly install it onto the device.

Organization XYZ-owned laptops can remotely connect to the organization's computer network to access files and systems such as timesheets, accounting and/or electronic databases. Laptops also have the capability to sync to other devices. This can pose confidentiality risks and the potential for a data breach if the laptop is not secure.

Policy Statement: Organization XYZ permits the use of Organization XYZ-owned laptops by personnel while they are working offsite. The use of laptops that are not owned by Organization XYZ is not permitted for any work that includes the personal information of service users. This can breach the confidentiality of women, children, and youth accessing VAW shelters and transition houses and put their privacy and safety at risk.

7.1 Passwords

Procedures: All Organization XYZ laptops will be set up by the IT subcontractor and password protected. Personnel using Organization XYZ laptops must use their unique computer User ID login and password to access the laptop.

7.2 Security Software

Procedures: The Administration Manager and IT subcontractor will ensure that security software such as anti-malware software (including anti-virus and anti-spyware organizations) is downloaded on all Organization XYZ owned laptops and is regularly updated.

When needed, personnel are required to bring the laptop they are using onsite on an agreed upon date to allow the IT subcontractor to ensure that all organizations and software are up to date.

If personnel notice something suspicious or receive a virus warning or alert on their organization laptop; personnel will discontinue using the laptop and report a potential breach to their supervisor or Administration Manager immediately.

7.3 Accessing Wi-Fi

Procedures: Personnel will not connect to and use public Wi-Fi networks when working on files and documents that contain any personal information or sensitive details. This includes, but is not limited to, free Wi-Fi networks available in coffee shops, restaurants, airports, community centres, hotels, and libraries. These typically insecure networks are vulnerable to hacking or interception.

7.4 Webcam

Procedures: Webcams on laptops typically have a visible light that turns on when in use so that the user knows the webcam is on. However, it is possible on some laptops to disable the light from turning on. Personnel at Organization XYZ will turn off the webcam when not in use. All Organization XYZ's laptops will have a cover on their webcam (e.g. removable sticker, post-it note, tape) when not in use.

Webcams will be positioned so that the location of the computer does not inadvertently reveal any potentially identifying and confidential information such as the location of the organization or reveal the identity of service users.

The Administration Manager in conjunction with the IT subcontractor and Executive Director will ensure that anti-virus, anti-spyware, and anti-malware systems are set up to scan Organization XYZ's computers regularly.

7.5 Logging into Organization XYZ's Computer Network Remotely (VPN)

Procedures: Personnel will log into Organization XYZ's virtual network by using their unique User ID log in and password.

When using organization owned laptops in public spaces, personnel will:

- Position the laptop in such a way that confidential information cannot be breached (e.g. by others able to read over their shoulder or from the next table)
- Not access free public wireless connections when working on confidential service user information

7.6 Connection to Other Devices

Procedures: Many laptops have the capacity to sync with other devices such as MacBooks, iPads, iPhones, and Apple watches. Personnel will ensure that their organization-owned laptop is not linked to any other devices whether they are work related or personal. They will do this by not inputting their personal User ID into a work laptop. This will make the laptop more secure and prevent inadvertent disclosure of any personal information. Personnel can do this by creating a specific User ID (e.g. Apple ID) for work laptops only and not using this ID with any other device.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

8. Tablet Owned by the Organization

Rationale: Tablets can make it easier for personnel to do their work while working offsite. Tablets can help personnel access files from the office, access email, and update any paperwork or reports. Though their size and portability can be

convenient, using tablets that are not owned by Organization XYZ can breach the confidentiality of women, children, and youth accessing the VAW shelter or transition house and put their privacy and safety at risk.

Unlike a computer that is set up in a specific location, tablets can be easily stolen or misplaced. It is also very easy for others to pick up a tablet and scroll through the information, which could include the personally identifying information of women, children, and youth accessing the shelter organization.

Many tablets have the capacity to sync with other devices (e.g. iPads, iPhones, MacBooks, and Apple watches). Tablets also allow users to download all kinds of spplications (apps). Some apps give developers access to the tablet, including access to an individual's personal information, contacts, communication, and photos. If service user information is stored in email, contacts, or other areas in the device, it might be possible for the information to be accessed by these apps.

Avoiding the use of non-organization tablets will help to protect service users, personnel, and Organization XYZ from subpoenas and breach of confidentiality legal action. This will make the tablet more secure and prevent inadvertent disclosure of any personal information.

Policy Statement: Organization XYZ allows the use of Organization XYZ-owned tablets by personnel while they are working offsite. In accordance with the guidelines provided by the Office of the Privacy Commissioner of Canada and (enter local privacy office here), using tablets not owned by Organization XYZ to communicate with service users is prohibited.

8.1 Account Set Up

Procedures: Some tablets require an account to fully operate. The Administration Manager and IT subcontractor will set up a general organization account for the tablet such as an organization username and ID if necessary and store the information in a locked cabinet on site. personnel must not use their personal accounts on organization-owned tablets.

8.2 Passwords

Procedures: All Organization XYZ-owned tablets are set up with a 4–6-digit security passcode by the Administration Manager and/or IT subcontractor. personnel will receive the passcode when signing out the tablet. Each personnel's password will be given to the supervisor or Administration

Manager in a sealed envelope, kept in a locked cabinet, and only accessed if necessary.

8.3 Storing Contacts

Procedures: Personnel will not save or store any past or present service user's contact information on Organization XYZ-owned tablets.

Names of Organization XYZ personnel can be stored on the phone's contact list on a first name basis only.

8.4 Personal Use

Procedures: When Organization XYZ loans a tablet to personnel to use for work purposes, Organization XYZ will communicate clearly all policies related to personal use of the organization tablet. These include policies related to:

- Storage of personal contact information
- Taking personal photos or videos
- Downloading apps
- Connecting to other devices
- Location tracking/GPS enabling functions
- Sending and receiving of personal communications

8.5 Ownership and Privacy

Procedures: By law, Organization XYZ must ensure personnel are following the policies outlined in this document and storing and destroying personal information in compliance with *(insert local privacy law)*. If necessary, personnel may be asked to provide their organization owned tablet to review security updates and confirm that deletion of communications are up to date.

According to some privacy commissioners like the OIPC BC, personal information in an organization's control may be subject to reasonable and acceptable corporate monitoring.

8.6 Sharing Location and Content

Procedures: Personnel will ensure that location services are turned off on their organization tablet when they are not using it.

Personnel will also disable Bluetooth capabilities on their organization tablet to minimize the risk of interception.

Note: If the location settings are turned on and personnel take a photo or video, the location, date, and time of where the photo/video was taken will be stored on the photo/video metadata (data of the photo).

8.7 Taking Photos and Videos

Procedures: Personnel will not take photos of any woman or child accessing the organization on Organization XYZ-owned tablets without their informed consent. Personnel will only take work-related photos and videos on their Organization XYZ owned tablets if necessary.

In compliance with (enter local privacy legislation here), personnel will inform service users of any risks associated with having their photo or video taken, such as risks when posting photos online and storing photos and videos on a cloud server, which makes it easy for third party interception.

Personnel will obtain written consent from service users using a *Photo Consent* form before taking any photos or videos. Service users will be informed that they have the right to withdraw their consent to use their image at any time.

8.8 Storing and Destroying Photos and Videos

Procedures: When setting up Organization XYZ-owned tablets and the accounts associated with it, the Administration Manager and IT subcontractor will ensure that photos and videos are not automatically backed up to any cloud servers including iCloud or Google Drive. When photos and videos are no longer needed, they will be downloaded onto Organization XYZ's main computer network and deleted off the tablet within three business days.

8.9 Cloud Backup

Procedures: When setting up Organization XYZ-owned tablets and the accounts associated with them, the Administration Manager and IT subcontractor will ensure that the tablets' content, including texts, emails, contacts, photos, and videos are not backed up to any cloud servers, including iCloud and Google Drive.

8.10 Connecting to Wi-Fi

Procedures: Personnel working on files and documents that contain any personal information or sensitive details or when communicating via email or Instant Messenger with service users, will not connect to or use public Wi-Fi networks. This includes, but is not limited to, free Wi-Fi networks available in coffee shops, restaurants, airports, community centers, hotels, and libraries. These typically insecure networks are vulnerable to hacking or interception.

8.11 Linking to Other Devices

Procedures: Personnel will ensure that their organization-owned tablet is not linked to any other work related or personal devices, neither work-related or personal.

8.12 Anti- Virus and Anti- Spyware

Procedures: The Administration Manager and IT subcontractor will ensure that security software or anti-malware software (including anti-virus software) are downloaded on all Organization XYZ-owned tablets and are regularly updated when new updates are available. If the tablets are being used offsite, personnel will be asked to return the tablets to the Administration Manager five business days in advance of the IT subcontractor performing an update.

8.13 Downloading of Apps

Procedures: Personnel must be cautious of the types of apps that are downloaded onto Organization XYZ tablets and fully read the Terms and Conditions of each app before they download. Personnel will only download apps that are necessary for their work. Personnel will pay close attention to what data these apps are accessing and collecting by reading the permissions, either on the device or on the apps' websites before downloading them to their work tablet.

If personnel have any doubt, they will check with a supervisor, Administration Manager, and/or IT subcontractor before downloading an app.

8.14 Updating the Tablet

Procedures: One easy security precaution to keep the tablet secure is to update the operating system with the latest versions. Personnel at Organization XYZ will download all available updates to their devices within five business days of the newest update available.

8.15 Remotely Wiping or Disabling a Phone

Procedures: A copy of the tablet account information and passwords will be left onsite with the Administration Manager, Supervisor, or Executive Director in case the Organization XYZ-owned tablet is stolen or misplaced. If the tablet is stolen or misplaced, personnel will report this to their supervisor immediately. The supervisor will contact the Administration Manager who will then connect with the IT subcontractor to assist in remotely disabling (locking the tablet from further use) or wiping (erasing the tablet's contents) the tablet in case any personally identifying information of service users is on the tablet.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

9. Cameras

9.1 Security Cameras

Rationale: Security cameras which record video are often necessary to help to maintain the safety of personnel and women, children, and youth accessing Organization XYZ services. They help personnel to identify who is accessing services and ensure it is safe to answer the door.

Policy Statement: Organization XYZ has security cameras that are placed both indoor and outdoor and are used to monitor the common areas of the shelter. In compliance with (enter local privacy act here), personnel will ensure that all current and potential service users are informed of:

- Security cameras on site and their recording range
- How long the recordings are stored for
- The fact that these recordings can be turned over to law enforcement if subpoenaed

Procedures:

a) Orientation and Intake: Recordings from a security camera are like any other personal data collected by organizations. In accordance with (enter privacy act here), Organization XYZ is required to receive informed consent when recording service users. Therefore, before a woman receives services, personnel must inform participants:
   - That security cameras are onsite
   - How long the recording is stored for
   - That with a subpoena, these recordings can be turned over to law enforcement

   Security camera video recording disclaimers are included in Organization XYZ's *Informed Consent to Service* form and personnel must provide service users the opportunity to consent to recording.

b) Personnel: All personnel will be informed by their supervisor at their time of hiring that there is a likelihood that they will be recorded on security cameras while working at Organization XYZ. A *Photo Consent* form will be given to personnel at the time of hiring that explains the storage of the recordings, how long recordings are stored for and procedures for destruction of video recordings. If personnel choose to sign the *Photo Consent* form, it will be filed in their personnel file.

c) Opt-Out Policy: The Executive Director will determine an Opt-Out policy for personnel and service users who do not consent to be recorded.

d) Notification and Signage: To ensure transparency, visible notification through signs and information will be posted around Organization XYZ to inform women, children, and youth accessing services that they are being recorded or viewed by cameras. Organization supervisors and the Executive Director will determine where and how many signs must be posted and in what languages with guidelines from the Office of the Privacy Commissioner of Canada.[5]

e) Storage of Recordings: In compliance with (enter local privacy act here), Organization XYZ will only keep video recordings for the shortest time necessary to address safety and security issues, for a maximum of one

[5] For more information, see OPCC's Guidelines for Overt Video Surveillance in the Private Sector https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gl_vs_080306/

year. The Executive Director, Administration Manager and IT subcontractor will determine the best way to store recordings and were.

f) Destruction of Security Camera Recordings: The Administration Manager, IT subcontractor, and the Executive Director will determine a plan to securely purge all camera images and recordings. In compliance with the guidelines offered by the Office of the Privacy Commissioner of Canada, Organization XYZ's recordings "should only be kept as long as necessary to fulfill the purpose of the video surveillance. Recordings no longer required should be destroyed. Organizations must ensure that the destruction is secure."

9.2 Cameras

Rationale: Like security cameras, cameras whether they use film, are digital or are part of a mobile phone, can store the personal information of personnel and service users.

Policy Statement: In compliance with (enter local privacy act here), personnel and women, children, and youth accessing shelter organizations will be given the option to consent to having their photo taken by being given a *Photo Consent* form before any photos are taken of them by personnel. No photos will be taken of personnel or organization participants without a signed copy of the *Photo Consent* form.

Procedures:

a) Informed Consent of Personnel: Personnel at Organization XYZ will be informed by their supervisor at the time of their hiring that there may be opportunities, such as organization events, where their photo may be taken. Personnel will be given the option to consent to having their photo taken by being given a *Photo Consent* form by the hiring supervisor. If personnel choose to sign the *Photo Consent* form, it will be filed in their personnel file.

b) Informed Consent of Service Users: Before taking photos or videos of women, children, and youth accessing the shelter or transition house, personnel will ask for permission and get informed consent through a *Photo Consent* form. The *Photo Consent* form will:
    - Have the date of the photo taken
    - State the purpose of the photo
    - Inform participants of where the photo will be stored
    - Inform participants how long the photo will be stored

- Inform participants of photo destruction policies.

Signed copies of a service user's *Photo Consent form* will be kept in her file.

c) Storage of Photos and Videos: Personnel taking photos or videos of Organization XYZ personnel or service users will transfer the images from the camera, video camera, or mobile device to the organization computer network within three business days. The photo/video will be deleted once transferred to the organization computer network or if it is determined not suitable for use.

If the photo(s)/video(s) are meant to be used later, personnel will upload ONLY the photos and/or videos that will be used to the organization computer network within three business days. All other photos and videos will be permanently deleted from the camera, video camera, or mobile device.

d) Destruction of Photos and Videos: After photos and videos (where consent has been obtained) are transferred via upload to the Organization XYZ's computer network, photos and videos will be permanently deleted from the device. Photos and videos will also be permanently deleted from any backup folders such as a "recently deleted" folder on an iPhone or a cloud-based storage system like iCloud immediately.

All photos and videos taken on organization cameras, video cameras, or mobile devices that are not needed will be permanently deleted from the device and any backup folders such as a "recently deleted" folder on an iPhone or on a cloud-based server like iCloud immediately.

Every year, the Executive Director and Administration Manager will set up a date and time to go through the photos and videos stored on the organization's server and delete unnecessary photos/videos.

e) Taking, Collecting, and Storing Photos and Videos for Evidence

Procedures: Personnel at Organization XYZ will not collect evidence (e.g. take photos of injuries). Alternatively, personnel will educate service users to safely collect their own evidence or have trusted friends and family support them in doing so, if they do not want law enforcement involved.

Because shelter organization records can be subpoenaed, personnel will not store any evidence for service users. Personnel will educate service users on safe ways to store evidence, such as creating a non-identifying email account (e.g. orangepeel@gmail.com) on a safe computer with a hard-to-guess password that they have never used before.

Personnel can link service users to legal support or law enforcement if further help is needed.

f) Recording Organization Delivery

Procedures: Personnel will not tape or video record any aspect of organization delivery (e.g. 1:1 session) with service users. According to *(insert local privacy law)*, any recording of a participant is considered part of their participant record. Any recording of a session (voice or video) will be considered part of a participant's record, which can be subpoenaed and can put participant's confidentiality and safety at risk.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

10. Electronic Databases

Rationale: Organization XYZ uses *(Organization XYZ to insert name of database)* database to electronically store the personal information of service users. Though using an electronic database can make record keeping practices easier, there are risks associated with the electronic storage of information, including compromising the personal information of service users. Therefore, personnel will only collect and store the minimal amount of personal information necessary to provide support services.

Policy Statement: Minimal, and only essential, information about service users will be entered into Organization XYZ's electronic database. All personnel will receive confidentiality and policy training about using Organization XYZ's database before entering personal information and case notes into the database.

10.1 User ID and Passwords

Procedures: Each personnel will be given a unique USER ID and password to enable them to enter the service user's personal information and case

notes into the database. This will help supervisors know who has accessed a service user's file should there be a breach or privacy violation.

Only personnel who have reason to access the database for shelter organization reasons will be given a User ID and password. personnel will access the database to input service user information and case notes.

10.2 Database Access

Procedures: Each personnel at Organization XYZ will access the database with their unique USER ID and password. personnel will be assigned an access level which enables them to only access records of the service users they are supporting. The database system can track each participant record that a particular USER ID views, inputs, updates, and changes. This will help maintain the privacy and confidentiality of service users.

10.3 Security Software

Procedures: The Administration Manager and IT subcontractor will ensure that all computers that have the capacity to access Organization XYZ's database are protected with firewalls and anti-virus, anti-spyware, and anti-malware software. These organizations will be updated once an update is available and will be completed within five business days of the release of the update.

10.4 Data Entry

Procedures: Organization XYZ's database is connected to the Internet. There is the potential for interception, a breach of data and/or a service user's information being susceptible to a subpoena. Therefore, minimal participant information will be entered. This means that only information that is necessary to provide shelter services, such as basic personal information of participants, will be entered. While being mindful of the woman, child, and youth's safety and what notes could support and undermine safety, only summarized case notes will be entered (e.g. Session 1: Focused on identifying feelings).

10.5 Subpoena of Data

Procedures: After receiving a subpoena for a service user's record, personnel will follow all steps outlined in Organization XYZ's electronic database policy manual. If it is determined that a service user's record must be submitted,

personnel will inform their supervisor and work to only print off and submit the record asked for in the subpoena.[6]

10.6 Destruction of Records

Procedures: In compliance with (enter local privacy act here), **Organization XYZ's** Executive Director will work with the database developer to ensure the permanent deletion of records. For VAW women's shelters and transition houses, it is recommended that service user records be purged seven years after the file is closed or seven years after the minor has reached the age of maturity.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

For more information about policies related to databases, please see WSC's Database Considerations for Anti-Violence Organizations.

[6] For more information see the BCSTH Legal Toolkit section on "Responding to Subpoenas and Record Requests," https://bcsth.ca/projects/legal-education-resources.

Section 2: Online Communication

1. Texting

Rationale: Texting can be a convenient way to communicate with service users, particularly those who are Deaf or hard of hearing. However, because of the potential for mobile phones to be monitored (e.g. by abusive current and former partners), communicating via text can put a participant's safety at risk. Personnel must consider the safety of participants before using text as a method of communication.

Policy Statement: Organization XYZ supports accessible communication between personnel and (past or current) service users if it is safe to do so. Personnel will only text service users (once consent has been given by the service user) with Organization XYZ-owned mobile phones *only*. Personnel who text with service users on mobile devices owned by Organization XYZ will comply with the informed consent, storage, and destruction of personal information policies that are in compliance with (enter local privacy act here) (See Policy 2: Mobile Phones Owned by Organization on page 8).

Because the definition of "record" is broad and can include all telecommunication with participants (e.g. texts, emails, instant messages), Organization XYZ requires all personnel to follow the following policies to prevent any inadvertent disclosure of confidential personal information that can also be at risk of a subpoena.

1.1 Texting Shelter Organization Colleagues

Procedures: Personnel communicating via text with other Organization XYZ personnel using organization-owned mobile devices will not text any personally identifying information about a service user.

Personnel will not store the full name of Organization XYZ personnel in the contacts of their mobile device.

1.2 Texting Service Users

Procedures: Before communicating via text with service users, personnel at Organization XYZ must discuss with participants their preferred methods of communication and discuss any risks to privacy and safety. Service users should be informed that if the perpetrator owns the phone and/or account, shares the phone account such as an iPhone account or if the phone is

connected to another device such as a laptop or tablet, that texting or calling from that phone may not be a safe or confidential option.

Boundaries about texting or other online forms of communication (e.g. instant messaging) will be discussed prior to texting service users. personnel will inform service users that texting will be used only for general purposes such as appointment reminders, and not for counselling.

Personnel will also inform service users:

- The office hours that they and other personnel are available
- That their text will be returned within 2-3 business days as they are not available 24/7
- Alternative people to reach out to when they are not available
- What can and can't be discussed via text
- Safety code words

Once service users are informed of any risks, they can decide if texting with personnel is a safe option.

Personnel will receive written, time-limited, informed consent from a service user before texting by asking the service user to consent to Organization XYZ's *Consent to Communicate via Technology* form. Personnel will only text general information with service users. No personal information or communication that could be harmful to a participant will be discussed. Personnel must consider the risks if either device was being monitored, was lost or stolen, or subpoenaed. All text communication is considered part of a service user's record and contents of the text must be included in a subpoena.

1.3 Deleting Text Logs

Procedures: Personnel with an organization-owned mobile phone will delete the mobile phone's call log, text message log, and voicemails daily unless it is necessary to keep (e.g. it is evidence). Keeping a text message, photo, email, or voicemail from a potential or existing service user should only be done so with permission from a supervisor, and/or when necessary, the Executive Director. Communication may also need to be kept if a subpoena for a service user's record has been received.

1.4 Storing Service User Contact Information

Procedures: Personnel will not store service user contact information in their organization owned mobile device. Service user's contact information includes, but is not limited to, first and last name, phone number(s), email addresses, home addresses, school information, photos, and/or social media user IDs.

1.5 Developing a Texting Safety Plan

Procedures: After receiving informed consent to begin communicating with service users via text, personnel at Organization XYZ will safety plan with the service users about possible safety risks. Key discussions will take place around:

a) Caller ID: When communicating via text, mobile phone carriers do not block or show the phone numbers as private. Therefore, anyone monitoring a service user's phone will see the mobile phone number that personnel are texting from. Personnel can suggest sending a code word or phrase to use with each other before communicating any confidential information via text.

b) Impersonation: It is easy for a perpetrator to impersonate a service user, especially if the perpetrator is the owner of the phone and has access to the account. Personnel can suggest that they share a code word or code name with the service user that the service user must answer before continuing a conversation with them.

c) Storing personnel Information: Personnel can request that the service user not store their contact number, including their name, in the service user's contacts. Personnel can suggest a general alternative name or business to store the support worker's phone number under so that she may not be questioned if the perpetrator is monitoring her phone.

d) Boundaries: Personnel will recommend an alternative number for the service user to call or text after hours, such as a 24-hour crisis line or 9-1-1. Personnel will be transparent in letting participants know that they are unavailable after their workday and that they may not respond for 2-3 business days.

Policy Creation Date:
Policy Review Date:

Policy Designate / Overseen by:

2. Email

Rationale: Many personnel use email daily in their work to communicate with service users directly or to coordinate services with other community organizations. Email, however, is not the safest way to communicate. Emails can be forwarded accidentally or intercepted by someone for whom the email was not intended.

Policy Statement: Organization XYZ is committed to communicating with women, children, and youth in the most accessible and safest way possible. For some service users, emailing may be the only method available to communicate, but for most a phone call may be safer. This is because the definition of "record" is broad and can include all forms of communication with service users (e.g., texts, emails, instant messages). Organization XYZ requires all personnel to comply with the following policies to prevent any inadvertent disclosure of confidential personal information that can also be at risk of a subpoena. The following policy procedures apply to emailing with service users on all devices.

2.1 Assessing Women's Safety before Emailing

Procedures: Personnel will follow email best practice and assess any potential safety risks before emailing or replying to an email from a service user.

a) Personnel will only communicate with (past, current, or potential) service users using an Organization XYZ email address. Personnel will not use their personal email to communicate with service users.

b) Personnel will confirm with service users if it is safe to email them. This will include, but is not limited to, asking:
   - Does the perpetrator have access to their email and knows their password?
   - Is the device that she checks her email on connected to another account or device (e.g. does her email come up on her iPhone, iPad, Apple Watch, and/or MacBook)?
   - Is the perpetrator tech savvy or is there any reason to believe that her online activity is being monitored?

If the service user has answered yes to any of the above questions, suggest that the service user:

- Open a new email account on a "safe" computer that the perpetrator does not have access to and create a new unique password that would be difficult for someone to guess.
- Include a code word in her emails so that personnel know that she is not being impersonated by her perpetrator or anyone else.
- Discuss email safety and privacy with service users, encouraging them to delete their sent messages from both their sent and deleted folders if they are concerned that their account could be accessed by someone else.

c) Personnel will not store a service user's email address in their personal and/or organization email address book or mobile device contacts.

d) To prevent sending emails to the wrong person, personnel will always double-check that the email address is correct. Most email organizations will "autofill" the rest of the address after the first few letters of the name are typed in.

e) If personnel must print out an email exchange, shred the email conversation as soon as it is no longer needed.

f) Personnel will delete any emails from service users once they have finished reading the email. Emails will be double deleted by opening the "Deleted Items" folder on the device and deleting the email to ensure it is not stored in the device's email organization.

2.2 Responding to Service Users Emails

Procedures: Personnel will always delete the previous conversation thread when responding to emails from service users. This ensures that if an email accidentally gets forwarded, intercepted, or if the account is accessed by the perpetrator, the entire history of the conversation isn't revealed.

Personnel will also:

- Ensure that the subject line in the email is something general
- Only communicate with participants using their Organization XYZ email address

- Refrain from sending emails to service users from their personal email address.

2.3 Deleting Emails from an Inbox and Delete Folder

Procedures: Because emails are considered part of a service users record, personnel will delete emails from service users as soon as they have been read to not keep identifying information longer than needed. This includes purging the "sent" and "deleted" folders as well.

2.4 Accessing Email Remotely

Procedures: Personnel have the capacity to access their email when working offsite. Personnel wishing to access their email remotely will be given a *User Agreement* form by their supervisor outlining monitoring practices. In accordance with *(insert local privacy law)*, the following procedures will take place before accessing email remotely:

a) Approval from a supervisor or Executive Director is needed to access emails remotely. Approval will largely depend on whether this capability is needed for personnel to do their job.

   Supervisors will consider:

   - The need to access email remotely to ensure personnel are not checking and responding to email on their off time
   - Whether the mobile device being used is an organization-owned device
   - If the device is not an organization-owned device:
     - Who has access to the mobile device?
     - Is the mobile device password-protected?
     - Are any accounts such as an Apple/Google ID shared or used on multiple devices?
     - Is the mobile device connected to other mobile devices?
   - How is the phone backed up? (e.g. is the phone automatically set up to back up to iCloud or another cloud-based service?)

b) All devices considered for accessing email remotely (e.g. computer, laptop, tablet, mobile phone, watch) must be password-protected.

c) All devices in which email will be accessed remotely will have their geo-tracking (i.e. location) settings turned off when not in use.

d) Personnel will know which apps can access information from their phone, including from their work email.

2.5 Corporate Monitoring of Devices

Procedures: In accordance with *(insert local privacy law)*, if personnel communicate with service users via online communication (e.g. through remote email, texting, and instant messaging) and if there are any concerns by their supervisor or Executive Director over the online communications, Organization XYZ personnel will be subject to reasonable and acceptable monitoring of the device (either organization-owned or a personal device). Personnel wishing to access their email remotely will be given a *User Agreement* form by their supervisor outlining monitoring practices. Personnel will refer to Organization XYZ's Operational Policy for more information.

2.6 Email Back-Up to Third Party Cloud

Procedures: In accordance with *(insert local privacy law)*, Organization XYZ's Administration Manager or IT subcontractor will check regularly to ensure that their organizational email is not being automatically backed up to a third-party cloud server other than the one that is set up by Organization XYZ. If personnel suspect that their email is being backed up to a third-party cloud server, they will notify their supervisor as soon as possible.

2.7 Internal Communication about Service Users

Procedure: Internal communication via email about service users is restricted. personnel will not include names of service users or other personal identifying information in emails.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

3. Social Media

Rationale: Organization XYZ uses Social Media platforms such as (*insert relevant platforms)* to raise awareness about the organization, increase dialogue and share their collective voice supporting women, children, and youth experiencing

violence. Responding to opposing views, negative and harmful comments, or blatant inaccuracies are issues with which many organizations struggle. It is important to have a policy beforehand so personnel can address it with confidence and clarity. Having a clear purpose for why Organization XYZ uses social media will help the organization develop policies around responding to opposing or negative views.

Policy Statement: Personnel will never post service user information and images or non-public domestic violence or sexual violence accounts on Organization XYZ social media accounts as this may reveal the identity of women, children, and youth accessing services and violate their confidentiality.

3.1 Access to Organization Social Media Accounts

Procedures: ORGANIZATION XYZ's social media accounts will be administered by the following organization positions: *(Organization XYZ to insert)*

Organization XYZ's personnel are welcome to "follow," "friend," or "like" Organization XYZ social media pages from their personal social media accounts if they have assessed the personal benefits and risks and if they feel comfortable and want to do so.

3.2 Posting about Service Users

Procedures: Personnel will never post personal information, including photos, videos, and concerns about past and present service users on their personal or Organization XYZ social media pages. This also includes, but is not limited to, commenting on service user's posts that could indicate that they are a past or present recipient of Organization XYZ services.

3.3 Posting about Organization XYZ Personnel

Procedures: Personnel will always receive informed consent from Board members, employees, subcontractors, service providers, volunteers, trainees, work placement, and student interns before posting pictures, images, and names on social media. The administrators of Organization XYZ's social media accounts *(See Section 3.1)* are responsible for obtaining permission from personnel, speakers, and attendees of community events before posting online.

If obtaining consent is not possible, offer clear and upfront notice about where a photo or video will be posted at the time of capturing to allow people to choose not to be in the photo or video frame.

3.4 Responding to Service Users Communicating via Social Media

Procedures: If a former, current, or potential service user reaches out for help via social media (through comments or private message), the social media account administrators will explain to the service user:

- To contact Organization XYZ's 24-hour help line
- If they are not able to call the 24-hour help line, the administrators will suggest alternative ways to contact the organization or another organization
- That Organization XYZ's social media accounts are accessible by multiple people and that the social media platform itself may store the information written in the conversation
- That some social media "chat" functions do not let the organization delete the messages they receive
- The potential safety and confidentiality risks when using social media
- That because the definition of "record" is broad and can include all communication with participants (e.g. texts, emails, instant messages), their online conversation could be used if her records were subpoenaed

If the platform allows, the social media administrators will do their best to delete the conversation(s) or message(s) on social media immediately after communicating with a service user.

Social media administrators will not respond to social media posts outside of office hours.

3.5 What to Post on Organization XYZ's Social Media Accounts

Procedures: Only social media account administrators (*See Section 3.1*) will post on Organization XYZ's social media accounts. When deciding what to post, social media account administrators may develop content guidelines. These guidelines will consider that:

- What they post on social media reflects Organization XYZ
- What they post should support Organization XYZ's communication goals. (e.g. if the social media pages are a way to showcase

Organization XYZ and its activities, their policy may say that they only post activities that Organization XYZ supports or is involved in. If Organization XYZ uses their social media pages as a platform to engage with others on broader anti-violence issues, they may post articles, videos, or events that are broader than the services or work their organization provides).

3.6 Responding to Opposing Views on Organization XYZ's Social Media Account

Procedures: Only social media account administrators (*See Section 3.1*) will respond to posts on Organization XYZ's social media accounts. Social media account administrators will decide whether and how they will respond to opposing views and ensure that their response reflects Organization XYZ's strategy and is grounded in its mission, vision, and media goals. If necessary, the social media account administrators will consult with their supervisor and/or Executive Director.

3.7 "Friending," "Liking," or "Following" Others on Organization XYZ's Social Media Account

Procedures: Organization XYZ will create a set of criteria to determine who they "friend," "like," or "follow" on social media. This set of criteria will take into consideration the information that Organization XYZ shares through its social network and whether it is appropriate to share that with the person who wants to join the organization network. If Organization XYZ uses social media to raise awareness and therefore wants to accept all "friend" or "follow" requests, it is important that the organization is constantly reviewing the information on its social media account to ensure that it's appropriate for a broad audience.

3.8 Responding to Inappropriate Content on Organization XYZ Social Media Account

Procedures: Only social media account administrators will respond to or delete posts on Organization XYZ's social media accounts. Organization XYZ will inform users of their rules for engagement on their social media account.

If social media account administrators remove any posts or comments from their social media account, they will have clear guidance around why and how they will remove them. They may consult with their supervisor or

Executive Director if necessary. Any posts or comments that include personal information will be deleted. Comments or posts that are blatantly inaccurate, harassing, or meant to cause harm will also be deleted.

Social media account administrators may consider informing the person whose comments or posts were removed about why they were removed and remind them of Organization XYZ's content guidelines.

3.9 Social Media Monitoring and Oversight

Procedures: Organization XYZ will have clear guidelines on who monitors and oversees their social media accounts. These guidelines will also define how much time is spent managing the accounts. The guidelines will reflect:

- What level of engagement Organization XYZ wants to have online
- How much oversight is preferred over the social media accounts
- How often social media account administrators will monitor comments and posts
- The amount of time social media account administrators spend on social media accounts (e.g. If social media account administrators have limited hours to spend on social media, Organization XYZ may decide to turn off the feature that enables comments or have clear rules of engagement for members)

Note: Organizations should also consider adding policies about the use of personal social media during work hours.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

4. Video Chat

Rationale: Video chat (e.g. Zoom or Facetime) can be a convenient way to communicate with former or current service users, if it is safe to do so.

Policy Statement: Personnel at Organization XYZ who have received a request from a service user to communicate via video chat will seek permission from their supervisor and ensure that the technology platform they are planning on using is safe, owned by Organization XYZ and has IT security up to date. Personnel will only use organizational accounts for video chat. If the supervisor is unsure whether the technology complies with *(insert local privacy law)*, they will request support from the IT subcontractor.

4.1 Assessing Risk

Procedures: Before asking for permission from their supervisor to provide service delivery via video chat with a woman accessing the shelter or transition house, personnel must assess for safety risks associated with using video chat.

Personnel will begin assessing risk by asking the organization participant:

- What device do they plan to use to video chat?
- Does the device have an up-to-date anti-virus organization running?
- Does the perpetrator have access to the device?
- Is the perpetrator tech savvy?
- Does she have reason to believe that her device is being monitored? Explain the potential risks to her safety.
- Is the video chat account used by more than one person?
- Is the device that is being used for the video chat used by more than one person?
- Is the account accessible to or connected to other devices?
- Is the video chat account password protected?
- Does the perpetrator have access to the video chat account?
- Does the perpetrator live at the home where the organization participant will be chatting?

If the service user answers yes to any of the above questions, personnel will discuss whether it is safe to communicate with this service user online with a supervisor. Developing a safety plan prior to video chat may need to be accomplished first.

4.2 Technology Safety Planning before Communicating via Video Chat

Procedure: If the request to video chat with a participant is approved, personnel at Organization XYZ must safety plan with the service user before communicating via video chat.

Safety planning with the service user will include:

- Advising the service user to not save Organization XYZ's contact information on the device or in the chat organization
- Ensuring that the device is used in a private location
- Creating a plan or code word that the service user will use if the chat is interrupted or disconnected

- Informing the service user that personnel cannot participate in video chat if she wishes to record the chat

Prior to beginning a video chat, personnel will:

- Inform service users of any potential risks of video chat
- Get the service user's informed consent to access service via video chat using the *Informed Consent* form

4.3 Personnel Video Chat

Procedures: Personnel at Organization XYZ planning to video chat with participants will ensure that:

- The device they will be using is an organization-owned device
- The device has the most up to date anti-virus software
- The video chat will only take place on an organization site or in a location where no one can overhear the session and will not capture any other service user accessing Organization XYZ services
- They will use a video chat account set up with their organization work email
- They will not save the service user's username or account in the video chat contact list
- They will delete any instant message chats and other information about the video chat that may be saved on the video chat platform
- They will delete the history and/or call log immediately after the chat
- The video chat is not recorded
- They discontinue the chat if the participant wants to record the chat session

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

Section 3: Organization Technology

1. Website Safety

Rationale: Organization XYZ has a website to share information about services and to raise awareness about organization organizations available to support women, children, and youth experiencing violence. As many perpetrators monitor survivors' online activities, whether through looking over their shoulder, manually going through their Internet browsing history, or via computer or mobile phone monitoring software, the website will be designed with this in mind and promote women's online safety.

Policy Statement: Organization XYZ is committed to ensuring that its website is as accessible and as safe as possible for visitors.

1.1 Safety Alert

Procedures: Organization XYZ's Executive Director, Administration Manager, and IT subcontractors will ensure that there is always a safety alert on the organization's website to remind visitors that their activities could be monitored or viewed by someone who has access to the device. Counsellors will advise organization participants of these safety features.

1.2 Quick Escape Button

Procedures: Organization XYZ commits to having a quick escape button on its website which a visitor can click any time to be redirected to an innocuous webpage. Quick escape buttons will only prevent immediate over-the-shoulder monitoring, such as when the perpetrator walks in, and the visitor needs to quickly close a webpage. This button will not prevent the web browser from logging the webpage to the browsing history or pressing the "back" button. Personnel will advise service users of these safety features and their limitations.

1.3 Web Form

Procedures: Some women, children, and youth experiencing violence will want to email the shelter organization to ask for help or resources and will go to Organization XYZ's website for the contact information. As a web form offers more privacy for staff and does not leave a record of the email in the sender's email sent folder, Organization XYZ will use a web form where

visitors can send personnel their message. This message will be submitted as an email to personnel.

Personnel will advise service users of these safety features and their limitations, including that if the perpetrator is monitoring the computer with spyware, a web form will not conceal that they have reached out for help.

1.4 Limit Information of Service Users Online

Procedures: Organization XYZ commits to never posting any information, photos, or videos of women, children, and youth accessing shelter services on the organization website; except in unique circumstances (e.g. a community or organization event) and when informed consent has been given.

1.5 Posting of Personnel

Procedures: Personnel will obtain permission and written informed consent from Organization XYZ personnel before posting any names, photos, or videos of personnel on Organization XYZ's website.

1.6 Accurate Information

Procedures: Organization XYZ commits to posting only accurate information on the organization website. Organization XYZ will include information specific to service delivery, service delivery area and ensure that any links to resources or community partners are up to date and accurate. personnel will advise service users of these resources.

1.7 Accessibility

Procedures: Organization XYZ commits to ensuring that its website is accessible to all visitors, including those with low vision, and visitors who are blind, hard of hearing or deaf.

Organization XYZ will:

- Check that images on the organization website have alternative text descriptions (i.e. html alt text)
- Ensure that there is concise and descriptive text within each link (and within the html title tag) that describes where the link takes a visitor.

This will ensure that a visitor to the organization's site or page via a screen reader can listen to helpful and accurate information.
- Include captions or transcripts when posting video or audio, so those who are hard-of-hearing or deaf can also receive the information
- Use a font size of 12-16 points

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

2. Internet Use

Rationale: Having the Internet available gives personnel at Organization XYZ a tool to help provide organization services and empower service users to make steps towards living safely and independently from violence.

Procedures: Organization XYZ will provide personnel with the tools necessary to provide shelter organization services. This includes providing safe and secure access to the Internet.

2.1 Acceptable Use

Procedures: Service users will access the Internet by logging on to Organization XYZ computers using Guest login and passwords. Guest login and passwords will be provided by personnel.

If it comes to the attention of personnel that service users are accessing problematic sites, this will be reported to their supervisor. The supervisor will communicate with the Executive Director, who will decide whether the IT subcontractor should block certain content.

The Executive Director will work with the IT subcontractor to increase the privacy of service users by setting up:
- Guest logins
- Participant computers to limit the amount of information that web browsers collect. This includes but is not limited to:
  - Deleting Internet tracking, history and cookies
  - Site blocking
  - Disabling auto-complete features and login information
  - Disabling auto-save logins and passwords

Because service users are accessing a shared computer, personnel will:

- Suggest that service users browse in a private browsing window
- Inform participants of safety features that allow participants to browse privately so that others using the computer won't have access to browsing history, cookies, and information entered in forms (e.g. Google offers users to browse "incognito")
- Explain that downloads and bookmarks will be saved on the computer
- Explain that some of their activity will be able to be seen by Organization XYZ's IT subcontractor

2.2 Personal Use

Procedures: Personnel, while at work at Organization XYZ, can access the Internet for acceptable use during personal time. (*Organization XYZ to define terms of acceptable use*)

Policy created date:
Policy review date:
Policy designate / overseen by:

3. Data Plan Responsibility

Rationale: Best practices outlined by the Office of the Privacy Commissioner of Canada recommend that organization owned mobile devices (e.g. mobile phones, tablets, and laptops) are the mobile devices to be used by personnel when communicating with women, children, and youth accessing shelter organization services.

Policy Statement: As per recommendations from the Office of the Privacy Commissioner of Canada, only organization owned mobile devices are to be used when communicating with organization participants. Organization XYZ is responsible for paying the monthly and/or annual plan of the device and negotiating all contracts associated with the device.

Procedures:

a) Organization XYZ is responsible for the purchase and payment of organization-owned mobile devices. Organization XYZ will pay the negotiated rate and taxes in agreement with the mobile carrier. Any usage, such as data over usage or long-distance charges must be discussed with the organization supervisor. If these charges are due to personal use, it is the sole responsibility of the

personnel who have been granted use of the mobile device while employed at Organization XYZ to reimburse the organization for these charges. Organization XYZ will negotiate all terms and contracts for the mobile device.

b) Supplementation of Personnel Devices: Organization XYZ will not supplement the monthly fees of non-organization owned phones.

Section 4: Technology Security

1. Wi-Fi

Rationale: Wi-Fi connectivity can make connecting to the Internet at Organization XYZ more accessible for personnel and the women, children, and youth who access our services. Providing access to the Internet via Wi-Fi can be helpful for personnel to carry out their work on organization owned mobile devices. Having Wi-Fi accessible to women, children, and youth accessing shelter organizations can be empowering as service users increasingly need to access the Internet to stay connected to family and friends, find community resources, and look for affordable housing and employment.

Policy Statement: Organization XYZ's VAW shelter and transition house sites have Wi-Fi capacity. Because of the sensitive nature of the work done by personnel, access to Organization XYZ Wi-Fi by personnel and organization participants will only be allowed if security measures are in place.

1.1 Wi-Fi Network Set Up and Security Settings

Procedures: The Administration Manager, supervisor, Executive Director, and IT subcontractor will work together to ensure that Organization XYZ's shelter organization site's Wi-Fi is as secure as possible. The proper configurations will be in place to make sure that the organization Wi-Fi only supports the most up-to-date protocols for transmitting information including:

- The only security algorithm that should be enabled is WPA2. Disable WEP and WPA.
- The only encryption method that should be enabled is AES. Disable anything related to TKIP.
- Completely disable WPS. This feature is enabled by default on most Hotspots. It allows for an alternate method of connecting without the password. It has a significant security flaw that can be easily exploited.

If personnel notice any changes to these settings, they will contact the Administration Manager as soon as possible.

1.2 Wi-Fi Network and Guest Network

Procedures: Shelter sites will have a minimum of two Wi-Fi Networks. The Administration Manager, Executive Director, and IT subcontractor will set up a Wi-Fi network for Organization XYZ personnel use only. A second

Guest Wi-Fi network will be set up and available to service users in need of accessing the Internet. Personnel will give out the password to the Guest Wi-Fi network to service users at their discretion.

(Organization XYZ insert name of Wi-Fi network) Wi-Fi Network is for personnel ONLY to log in to while they are on site.

(Organization XYZ insert name of Wi-Fi network) is a Guest Wi-Fi Network for service users and Organization XYZ guests to log in to while they are on site.

1.3 Password Protection

Procedures: There are two Wi-Fi networks at Organization XYZ: one for personnel and one for service users. These two Wi-Fi networks will have two separate passwords, one for each network.

The Executive Director, Administration Manager, and IT subcontractor will ensure that these passwords are strong and kept in a secure location.

Supervisors will give the Wi-Fi network ID and password to personnel when needed. Because of the sensitive nature of domestic violence shelter work, personnel will not access the Internet through the Guest Wi-Fi network.

Personnel will only give the password to the Guest Wi-Fi network to participants and guests when needed/requested.

1.4 Accessing Wi-Fi Networks Offsite

Procedures: If personnel need to access Wi-Fi offsite for Organization XYZ related work, personnel will determine if the Wi-Fi network they are using is safe and secure enough for the work they are doing. If personnel are emailing participants, entering case notes, or video chatting with service users, they will not connect to free public Wi-Fi.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

Section 5: Additional Considerations

1. Information Technology Support

Rationale: As our use of technology increases, Organization XYZ subcontracts Information Technology (IT) work to *(Organization XYZ insert name of IT subcontractor)* who specializes in secure IT work.

Policy Statement: Organization XYZ is committed to ensuring that its IT is as safe and up to date as possible and will subcontract *(Organization XYZ insert name of IT subcontractor)* to do this. The Administration Manager and Executive Director will review the satisfaction of IT services annually.

1.1 IT Support

Procedures: When personnel at Organization XYZ need IT support, they will contact the Administration Manager who will contact the IT subcontractor and arrange a time to have the request serviced.

1.2 Satisfaction

Procedures: If for any reason personnel at Organization XYZ have questions or is not satisfied with the service they receive from the IT subcontractor, they will notify their supervisor and/or Administration Manager with their concerns.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

2. Accessibility

2.1 Using Technology to be More Accessible with Service Users

Rationale: A variety of technology is available to help personnel communicate with service users who may need extra support to access shelter services. Organization XYZ works to ensure that our services are accessible to any woman, child, or youth who needs them.

Policy Statement: Organization XYZ recognizes that under the Canadian Human Rights Act, it is against the law to discriminate on the basis of race,

national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability, pregnancy or childbirth, and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered. As such, Organization XYZ and its shelters/transition houses ensure that IT services and organizations are accessible to women, children, and youth. Organization XYZ will not practice or engage in unlawful discrimination based on culture, spiritual beliefs, gender identity, social condition, physical ability, and any prohibited ground of discrimination covered by the Canadian Human Rights Act as listed above. Organization XYZ will provide shelter services that are sensitive, responsive, and accessible to the diverse needs of the service users it serves and promote cross-cultural understanding, safety, and respect for diversity among participants and staff.

Procedures: During intake, personnel at Organization XYZ will assess if a service user needs extra support to access the shelter. If it is determined that one of the needs is to communicate using technology, personnel will consult with their supervisor to explore the best way to obtain assistive technology or translation services to reduce barriers to access women's shelter services.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

3. Purchasing

Rationale: It is important for personnel to have access to the appropriate technological tools needed to support service users.

Policy Statement: Organization XYZ is committed to supporting personnel to have the tools necessary, including access to technology tools, to provide services.

3.1 New Software Requests

Procedures: When the budget allows, Organization XYZ may purchase new software to enhance the services provided to service users.

When new software is needed, personnel will make a request to their supervisor who will then notify the Administration Manger, Finance Manager, Executive Director, and/or IT subcontractor.

3.2 New Hardware Requests

Procedures: When the budget allows, Organization XYZ may purchase new hardware devices to enhance the services provided to service users.

When new hardware is needed, personnel will make a request to their supervisor who will then notify the Administration Manger, Finance Manager, Executive Director, and/or IT subcontractor.

3.3 Applications for Mobile Devices

Procedures: Personnel at Organization XYZ may find that there are apps available to purchase through app stores that will enhance the services provided to service users.

Personnel wanting to purchase an app must do their due diligence and read the terms and conditions to ensure that the app:

- Will not monitor the content of the device (e.g. have access to the device camera, photos, contact lists, emails, and location)
- Will not sell the information gathered from the mobile device

A request to purchase the app must be made to the personnel's supervisor who will ensure that the app does not pose any potential risk by doing any of the above.

If the budget allows and the app is deemed low risk and necessary to provide service, it will be considered for purchase.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

4. Monitoring of Technology

4.1 Right to Monitor Technology

Rationale: Organization XYZ is transparent about its legal rights to monitor the technology used to provide service to service users.

Policy Statement: Organization XYZ is within its legal rights to monitor the technology used for shelter services that collect personal information of

participants (e.g. text, email). Organization XYZ is within its rights to "reasonable and acceptable corporate monitoring"[7] of an organization-owned device.

Procedures: When it has been deemed necessary to monitor organization-owned technology, Organization XYZ will define clear guidelines related to process, including how much time personnel will be given to turn over the device.

Guidelines will also define practices related to any investigations or litigation concerning information found on a device.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

5. Reporting Misuse

Rationale: Organization XYZ is committed to safe technology use and using technology in compliance with the Canadian Charter of Rights and Freedoms to preserve the privacy, confidentiality, and safety of women, children, and youth accessing the shelter or transition house.

Policy Statement: There may be times when personnel at Organization XYZ suspect that organization-owned technology or systems are being misused by personnel or service users. In a case where misuse of technology is suspected, the following processes will be followed.

5.1 Reporting Process

Procedures: If personnel suspect that organization-owned technology or systems are being misused by personnel or service users, personnel will notify their supervisor, Administration Manager, or Executive Director.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

[7]Office of the Privacy Commissioner of Canada. "Is a Bring Your Own Device (BYOD) organization the Right Choice for Your Organization?" https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/

6. Using a Personal Device for Shelter Services

Rationale: While using a personal device owned by personnel may be more convenient or cost effective, the Office of the Privacy Commissioner of Canada strongly recommends that an organization have a clear and fully operational Bring Your Own Device (BYOD)[8] plan in place that includes policy and training prior to any acceptable use of personal mobile devices. This is to ensure that the personnel of the organization comply with *(enter local privacy act here)*.

Policy: Organization XYZ prohibits the use of personally-owned devices (BYOD):

- When communicating with service users
- For the collection of personal information of service users

Procedures: Organization XYZ will create a *User Responsibilities* document that outlines:

- Acceptable and unacceptable uses of the BYOD and the collection of personal information of service users
- Employee functions and roles that are appropriate candidates for a BYOD organization
- Approved device, operating systems, operating system versions, and cloud services
- Clear policies and procedures about how personal information in an organization's control may be subject to reasonable and acceptable corporate monitoring on a BYOD device, and how BYOD users are informed of these monitoring practices
- Clear policies about the sharing of devices with family members or friends and the consequences of inadvertent disclosure of information
- Clear policies about application (app) management
- Clear policies about data and voice plan responsibility
- Clear policies about device security requirements
- Clear policies about subpoena requests for records and what that means for information stored on a personal device
- Clear policies about the liability and consequences of subpoenas for information stored on a personal device and the financial responsibility of legal fees

[8] For more information about BYOD policies see "Is a Bring Your Own Device (BYOD) Organization the Right Choice for Your Organization?" https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/ and Contemplating a Bring Your Own Device (BYOD) Organization? https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/tips_byod/

- Clear policies about whether geo-tracking information generated by the mobile device will be tracked by an organization
- Training on the collection, storage, and destruction of personal information as outlined by *(enter local privacy act here)* on the personal mobile device for all staff using their own device

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

Section 6: Service User Use of Technology

1. Shared Computers and Devices

Rationale: Providing service users access to shared computers at Organization XYZ enables and empowers service users to make steps towards living safely and independently from violence (e.g. searching for housing, applying for jobs and income assistance) and maintain connections with their support networks.

Policy Statement: When possible, Organization XYZ will provide shared computers for service users to use while they are accessing shelter services.

1.1 Use of Shared Computers

Procedures: Service users will access the Internet by logging on to Organization XYZ shared computers using Guest login and passwords. Guest login and passwords will be provided by personnel. The shared computer should not have access to Organization XYZ's shared drive or database.

Ideally, service users will use a separate computer from personnel that is participant-designated. However, if there is not a service user-designated computer and the service user must use a computer designated for personnel, personnel will log off and the service user will log in using the Guest login and password provided. This will ensure the security of Organization XYZ's computer network as well as the confidentiality and privacy of other participants.

If there is a service user-designated computer, the Executive Director will work with the IT subcontractor to increase the privacy of those using the shared computer by setting up:

- A guest account and login
- The shared computer in an area of the shelter that allows for privacy for the person using the computer and also privacy for other service users who may be inadvertently revealed if a computer camera or webcam is being used
- The Guest account without administrator rights, making it more difficult for anyone to download anything onto the computer without administrator permission
- So that it is not connected to the organization's computer network and consider disabling file sharing and the ability to remote access into these computers
- A removable webcam cover over the camera lens

- Shared computers to limit the amount of information that web browsers collect. This includes but is not limited to:
  - Deleting Internet tracking, history, and cookies
  - Site blocking
  - Disabling auto-complete features and login information
  - Disabling auto-save logins and passwords

Before service users use the shared computer, personnel will have a conversation with them that will include:

- Suggesting that they browse in a private browsing window
- Informing them of safety features that allow them to browse privately so that others using the computer won't have access to browsing history, cookies, and information entered in forms (e.g. Google offers users to browse "incognito")
- Explaining that downloads and bookmarks will be saved on the computer
- Reminding them not to save personal files or information on the shared computer
- Providing a portable USB drive when needed and available
- Explaining that some of their activity will be able to be seen by Organization XYZ's IT subcontractor

1.2 Internet Access on Shared Computers

Procedures: For service users to use the shared computer most effectively, Organization XYZ will provide organization participants with safe and secure access to the Internet. All browsers on shared computers will be set to the most private and secure settings.

1.3 Connecting to the Wi-Fi and Guest Network

Procedures: Organization XYZ will set up and provide a Guest Wi-Fi network available to service users in need of accessing the Internet. The Guest network will have a different network name and password than the one used by personnel. Shelter and transition house personnel will give out the password to the Guest Wi-Fi network at their discretion.

If there are any limitations to service users' use of the Wi-Fi, such as no streaming of videos or movies, personnel will be clear about the reasons for this (e.g. limited Internet bandwidth).

(Organization XYZ insert name of Wi-Fi network) is a Guest Wi-Fi Network for service users and Organization XYZ guests to log in to while they are onsite.

1.4 Blocking Content of Websites

Procedures: Organization XYZ can consider blocking potentially offensive content from web browsers on shared devices or networks by using the "parent controls" – keeping in mind that some service users may want or need to access websites that fall under "adult" content (e.g. sexual health websites).

If it comes to the attention of personnel that a service user is accessing problematic sites, a conversation can be had with the service user. If deemed appropriate, this will be reported to their supervisor. The supervisor will communicate with the Executive Director, who will decide whether the IT subcontractor should block certain content.

1.5 Security Software

Procedures: The Administration Manager in conjunction with the IT subcontractor and Executive Director will ensure that anti-virus, anti-spyware, and anti-malware systems are downloaded and set up to scan Organization XYZ's shared computers for service users regularly. Protect shared computers used by organization participants by keeping all anti-virus, anti-spyware, and anti-malware systems up to date and updating when new updates become available.

1.6 Data Storage

Procedures: When possible, Organization XYZ will provide service users with a USB drive to save their documents (e.g. resume, forms) on. Alternately, personnel can assist service users to set up a free "cloud" account for online storage. Discuss any privacy and safety concerns including perpetrators having access to the account and suggest creating and using a new email account, phone number, and/or profile picture that won't connect to previous accounts.

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

2. Service User's Personal Devices

Rationale: Most service users accessing Organization XYZ will have personal devices such as smartphones, tablets, and laptops. Though their size and portability can be convenient, there are security and confidentiality risks associated with using mobile phones and tablets that require careful consideration. For example, sometimes having the location settings turned on (under privacy settings) can be useful when a service user is finding directions to an appointment. Other times, having the location services turned on can inadvertently disclose their location, giving away the location of a confidential shelter location or the service user's address or school.

Other confidentiality and security risks to service users' privacy and organizational confidentiality to consider are that smartphones and tablets can:

- Easily be stolen or misplaced
- Breach personal information through contacts, call logs, emails, and text messages
- Quickly install spyware
- Have cloud servers easily accessed/intercepted for personal information, photos, and videos
- Inadvertently disclose personal information by linking to other devices
- Potentially enable third parties/developers to access personal information when downloading apps; some free applications may access other data stored on the device, such as contacts or pictures

Policy Statement: Service users accessing shelter services at Organization XYZ will be advised of the potential privacy and safety risks in using their personal devices.

2.1 Internet Access on Personal Devices

Procedures: For service users to stay connected to their support networks and manage responsibilities and tasks (e.g. searching for housing, employment) most effectively, Organization XYZ will provide service users with safe and secure access to the Internet.

2.2 Connecting to Wi-Fi and Guest Network

Procedures: Organization XYZ will set up and provide a Guest Wi-Fi network available to service users in need of accessing the Internet on their personal devices. The Guest network will have a different network name and

password than the one used by personnel. Personnel will give out the password to the Guest Wi-Fi network at their discretion.

If there are any limitations to service users' use of the Wi-Fi, such as no streaming of videos or movies, personnel will be clear about the reasons for this (e.g. limited Internet bandwidth).

(Organization XYZ insert name of Wi-Fi network) is a Guest Wi-Fi Network for service users and Organization XYZ guests to log in to while they are on site.

2.3 Sharing Location and Content

Procedures: Personnel will discuss possible safety risks related to location sharing and location tracking with service users and request that service users turn off their location services on their smart phones, tablets, and other devices that have location tracking when they are not using it.

Service users will also disable Bluetooth capabilities when not in use on their smart phones, tablets, and other devices to minimize the risk of interception.

Service users should also be informed that if the perpetrator owns the phone and/or account, shares the phone account such as an iPhone account, or if the phone is connected to another device such as a laptop or tablet, that texting or calling from that phone may not be a safe or confidential option.

Note: If the location settings are turned on and service users take a photo or video, the location, date, and time of where the photo/video was taken will be stored in the photo/video metadata (data of the photo).

2.4 Taking Photos and Videos

Procedures: Personnel at Organization XYZ will discuss the privacy and safety concerns related to service users taking photos or videos while accessing shelter services (e.g. inadvertently disclosing the location of the shelter, personnel, and/or other service users). All service users and personnel need to provide their full consent prior to having their photo and/or video taken and will be informed that they have the right to withdraw their consent to take their image at any time. Personnel will advise service users that storing photos or videos on a cloud server can

make it easy for unauthorized individuals to access and/or intercept personal images.

2.5 Gaming Consoles

Procedures: Personnel will discuss possible safety risks related to the use of gaming consoles with service users and their children and request that service users:

- Be alert to a player who asks for personal information, such as their address, location of the shelter, their name, email, or phone number
- Do not provide anyone with personal information such as their address, location of shelter, their name, email, or phone number
- Be careful when clicking on links within in-game chats, especially if they don't know the other gamer
- For games that ask permission to access the device's camera, microphone, or location data in order for the game to function properly, allow access while playing if deemed safe, but turn off access when not playing

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

3. Service User Online Communication

Rationale: For most service users, online communication will be their primary mode of communication while accessing the women's shelter or transition house. However, because of the potential for mobile phones to be monitored (e.g. by abusive current or former partners), communicating online can put a woman's safety at risk. Personnel will discuss the potential risks and safety considerations with service users to ensure they can make informed decisions about their online communication and also protect the safety of other service users and personnel (e.g. if the perpetrator owns the phone and/or account, shares the phone account such as an iPhone account, or if the phone is connected to another device such as a laptop or tablet, texting or calling from that phone may not be a safe or confidential option).

Policy Statement: Organization XYZ supports accessible online communication (e.g. text, email, social media, video chat) for service users if it is safe to do so and will provide all users with information about the risks related to online communication.

3.1 Social Media

Procedures: Personnel will request that service users not post photos, videos, or information about other service users or personnel on their social media accounts. These actions may violate the privacy and confidentiality of other service user, personnel, and the location of the organization, and could risk theirs and/or others' safety.

3.2 Video Chat

Procedures: Personnel will request that service users only video chat in a private location or in an area where there is no risk of violating the privacy and confidentiality of other service users and personnel, the location of the organization, or risk theirs and/or others' safety.

3.3 Webcams on Shared Computers

Procedures: Devices with webcams typically have a visible light that turns on when in use so that the user knows it is on. However, it is possible on some devices to disable the light from turning on. Service users using shared computers at Organization XYZ will turn off the webcam when not in use. All shared computers at Organization XYZ will have a cover on their webcam (e.g. removable sticker, post-it note, tape).

To reduce the risk of a breach of privacy or confidentiality, on Organization XYZ shared computers, personnel will:

- Ensure that the shared computer is in an area of the shelter that allows for privacy. If the computer has a webcam or built-in camera, set it up to ensure that if service users are using the webcam that no other person, or location information, is revealed when in use.
- Ensure that webcams on shared computers will be positioned so that potentially identifying and confidential information such as the location of Organization XYZ or the identity of service users is not inadvertently revealed.
- Place a removable webcam cover over the camera lens on the shared computer when the camera is not in use to prevent inadvertently revealing service users or if the camera gets turned on unintentionally.

3.4 Webcams on Service Users' Personal Devices

Procedures: Personnel will discuss possible safety risks related to webcam use with service users and request that service users using their own personal devices turn off the webcam when not in use. Devices with

webcams typically have a visible light that turns on when in use so that the user knows the webcam is on. However, it is possible on some devices to disable the light from turning on.

To reduce the risk of a breach of privacy or confidentiality, when service users are using the webcam on personal devices, service users will be asked to:

- Only use their webcam in the privacy of their own room and when no other service users or personnel are around
- Turn off their webcam when it is not in use

Policy Creation Date:
Policy Review Date:
Policy Designate / Overseen by:

References

- BC Human Rights Code, BC, "BC Human Rights Code." https://www2.gov.bc.ca/gov/content/justice/human-rights/human-rights-protection Retrieved January 28, 2019.
- Government of Canada. "Canadian Human Rights Act." https://laws-lois.justice.gc.ca/eng/acts/h-6/ Retrieved January 10, 2019.
- National Network to End Domestic Violence, Safety Net Project. "Organization's Use of Technology Best Practices & Policies Toolkit." https://www.techsafety.org/resources-organizationuse Retrieved February 7, 2018.
- Office of the Privacy Commissioner of Canada. "Contemplating a Bring Your Own Device (BYOD) organization?" https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/tips_byod/ Retrieved January 28, 2019.
- Office of the Privacy Commissioner of Canada. "Is a Bring Your Own Device (BYOD) Organization the Right Choice for Your Organization?" https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/ Retrieved January 28, 2019.
- Ontario Association of Interval and Transition Houses. "A guide to policy development for feminist anti-violence organizations." https://endvaw.ca/wp-content/uploads/2016/05/Guide-to-Policy-Development-for-Feminist-Anti-Violence-Organizations-OAITH-2010.pdf Retrieved February 22, 2019.
- Queens Printer. "Personal Information Protection Act." http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01 Retrieved January 24, 2019.