Use of Technology Policy Template Guide

For BC's Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) Programs for Children and Youth Experiencing Violence

BC Society of Transition Houses

ACKNOWLEDGEMENTS

Written by: Rhiannon Wong
Edited by: Louise Godard and Tanyss Knowles
Design by: Hannah Lee

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

Sections from this guide have been adapted from and developed in cooperation with the Safety Net Technology Project at the National Network to End Domestic Violence, United States.

BCSTH gratefully acknowledges the funding and support of the Ministry of Public Safety and Solicitor General who made the development of this program policy template and guide possible.

TABLE OF CONTENTS

OVERVIEW

This guide offers sample policy templates to assist anti-violence organizations to develop specific "use of technology" policies for the Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) Programs for Children and Youth Experiencing Violence. PEACE programs were formerly named the Children Who Witness Abuse (CWWA) Programs.

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 women, youth and children 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), sub-contractors, service providers, volunteers, trainees, and work placement and student interns working within the PEACE program.

The policy templates included in this guide reflect:

- contractual obligations by the Ministry of Public Safety and Solicitor General
- current legislation; and
- use of technology best practice.

The policy templates provided are meant to supplement current organizational, and specific PEACE Program, policies[1]. 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 PEACE program can use technology in a way that is attentive to the safety and privacy of women, children and youth that access PEACE programs.

PEACE program personnel and administrators are encouraged to review these templates and adapt them to the technology available to their PEACE programs. For example, in this guide, sample polices for fax machines, scanners and printers are written as if PEACE programs have three separate devices. However we know that many programs use "all in one" devices and, therefore, these policies can be combined in a way that makes sense for your organization.

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

[1] An online copy of the "PEACE Program Policy and Template Guide" can be found at https://bcsth.ca/wp-content/uploads/2018/05/PEACE-Program-Policy-Template-and-Guide-2018-Final.pdf

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 created 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 agencies depending on when the policy is implemented.

A NOTE ON LANGUAGE

Throughout this policy, we refer to program participants and women, children and youth accessing services. These terms are interchangeable.

Personnel refers to board members, employees (including the Executive Director and PEACE program counsellors), sub-contractors, service providers, volunteers, trainees, and work placement and student interns working as part of the PEACE program.

Personal information is defined by the Office of the Information and Privacy Commissioner for British Columbia in the Personal Information Protection Act (PIPA) as "information that can identify an individual" (for example, a person's name, home address, home phone number or ID number). It also means "information about an identifiable individual" (for example, physical description, educational qualifications or blood type). Personal information includes "employee personal information but does not include business contact information or work product information.[2]"

[2] Office of the Privacy Commissioner for British Columbia. (2015). A Guide to B.C.'s Personal Information Protection Act. https://www.oipc.bc.ca/guidance-documents/1438

SECTION 1: OFFICE TECHNOLOGY

1. Office Phones

Rationale: Agency XYZ[3] is committed to ensuring that all women, children and youth experiencing domestic violence are able to communicate with PEACE program 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 PEACE programs will communicate with women, children and youth in the safest, and most accessible method that **Agency XYZ** can provide based on resources and guidelines outlined by PIPA 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: Agency XYZ's landline phone system is set up to block the agency's phone number and name from showing up on the receiver's caller ID. If PEACE program personnel are in doubt, they will test the system before making a call to (potential) program participants.

If PEACE program personnel are calling a program participant 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. PEACE program personnel may unblock the agency's blocked number once they have:

- explained any potential safety risks, such as a perpetrator monitoring her phone call log and
- have consent from the program participant that it is safe to unblock the number when calling her.

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

[3] When writing their organizational polices, organizations will insert their own agency name in place of 'Agency XYZ'.

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

Note: Agencies 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 Voice Mail

Procedures:

a) **Password:** PEACE program personnel who have been assigned a voice mailbox will reset the password of the voicemail box when beginning their employment at **Agency XYZ.**

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

c) **Deleting Messages:** After listening to voice mail messages, personnel will immediately delete messages. This will be done unless the message is needed and the reasons are documented by the PEACE program supervisor.

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

2. Mobile Phones Owned by the Agency

Rationale: Agency XYZ is committed to having safe and accessible technologies available for personnel to provide PEACE program services. Mobile phones including smartphones can make it easier for PEACE program personnel to do their work while working offsite. Mobile phones can help PEACE program personnel communicate with fellow employees and program participants, check calendars, access files from the agency 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 phones privacy settings) can be useful, for example, to get directions when accompanying a program participant to an appointment. Other times having the location services turned on can inadvertently disclose the location of PEACE program personnel and participants, giving away the location of a confidential Transition House location or a program participant's address or school.

Other confidentiality and security risks to program participant's privacy and agency 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 party/developers to access personal information when downloading App's. This is because some free applications may access other data stored on the device, such as contacts or pictures.

Not using personal mobile phones will help to protect program participants, PEACE program personnel and **Agency XYZ** from subpoenas and breach of confidentiality legal action as all communication can be considered part of a program participant record.

Policy Statement: Agency XYZ allows the use of **Agency XYZ** owned mobile phones by PEACE program personnel while they are working offsite, with limitations. All personnel using agency mobile phones will be made aware of the potential safety and security risks (e.g. downloading of App's, cloud server storage) associated with mobile phones and the corresponding policies.

Using mobile phones that are not owned by **Agency XYZ** can breach the confidentiality of women, children and youth accessing the PEACE program and put their privacy and safety at risk. In accordance with the guidelines provided by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for BC, using mobile phones not owned by **Agency XYZ** to communicate with program participants is prohibited.

Note: Organizations allowing the use of personal laptops and mobile phones for PEACE program work must comply with the Office of the Privacy Commissioner and PIPA guidelines. Please see the Bring Your Own Device Section on page 59.

2.1 Program Personnel Accounts

Procedures: When **Agency XYZ** loans a mobile phone to a PEACE program personnel to use for work purposes, the PEACE program 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 **Agency XYZ** loans a mobile phone to PEACE program personnel to use for work purposes, the PEACE program personnel will set up the phone with a unique and strong password. Each program 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: PEACE program personnel will not save or store any past or present PEACE program participant's contact information on **Agency XYZ** owned mobile phones. Names of **Agency XYZ** personnel can be stored on the phones contact list on a first name basis only.

2.4 Voicemail

Procedures:

a) **Password:** PEACE program personnel at **Agency 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 agency 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:** PEACE program personnel at **Agency XYZ** will clearly record a voicemail greeting, which 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 voice mail messages, PEACE program personnel will immediately delete all messages. This will be done unless the message is needed and the reasons are documented by the PEACE program supervisor.

2.5 Caller ID

Procedures: All **Agency XYZ** mobile phones will be set up to block the caller ID. If a mobile phone is not set up to block the number or show up as private, PEACE program personnel will manually dial *67 before they dial the number of any (potential) PEACE program participants.

Some receivers will reject calls with blocked numbers. PEACE program 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 program participant that it is safe to unblock the number when calling her.

If PEACE program 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 **Agency** XYZ loans a mobile phone to a PEACE program personnel to use for work purposes, **Agency XYZ** will communicate clearly all policies related to personal use of the agency mobile phone. These include policies related to:

- storage of personal contact information
- taking personal photos or videos
- downloading of Apps

- connecting to other devices
- location tracking/GPS enabling functions, and
- sending and receiving of personal communications.

2.7 Ownership and Privacy

Procedures: By law, **Agency XYZ** must ensure PEACE program personnel are following the policies outlined in this document and storing and destroying personal information in compliance with PIPA. If necessary, PEACE program personnel may be asked to provide their agency owned mobile phone to review security updates and confirm that deletion of communications are up to date.

According to the OIPC BC, personal information in an organizations control may be subject to reasonable and acceptable corporate monitoring.

2.8 Sharing: Location and Content

Procedures: PEACE program personnel will ensure that location services are turned off on their agency mobile phone when they are not using it.

PEACE program personnel will also disable Bluetooth capabilities on their agency mobile phone to minimize the risk of interception.

Note: If the location settings are turned on and PEACE program 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: PEACE program personnel will only take work related photos and videos on their **Agency XYZ** owned mobile phones. In compliance with PIPA, PEACE program personnel will inform program participants 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 the personal images.

PEACE program personnel will obtain written consent from program participants 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 **Agency 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 3 business days when they are no longer useful or once they have been uploaded to **Agency XYZ's** main computer network.

2.11 Cloud Backup

Procedures: When setting up **Agency 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. PEACE program personnel will not change these settings in order to protect their privacy and confidentiality of program participants.

2.12 Connecting to Wi-Fi

Procedures: If PEACE program personnel are working on files and documents that contain any personal information or sensitive details, PEACE program personnel will not connect 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: PEACE program personnel will ensure that the agency owned mobile phone is not linked to any other devices, work related or personal e.g. iPhones to iPads, MacBook's 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. PEACE program 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 and photos. PEACE program personnel must be cautious of the types of Apps that are downloaded onto agency phones and fully read the Terms and Conditions of each App that they do download. PEACE program 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. PEACE program personnel will pay close attention to what data these Apps are accessing and collecting by reading the permissions, either on the device or the App's website before downloading them to their work mobile.

If PEACE program 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, Voicemails

Procedures: In compliance with PIPA, PEACE program personnel at **Agency XYZ** will delete the mobile phone's call log, text message log, text messages and voicemails daily, unless it is absolutely necessary to keep. Keeping a text message, photo, email, voicemail from a (potential) PEACE program participant 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 subpoenaed and considered part of program participant's record.

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

Agency XYZ owned phone is stolen or misplaced. If the phone is stolen or misplaced, PEACE program 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 program participants are on the phone.

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

3. Fax Machine

Rationale: Agency XYZ is committed to protecting the privacy and confidentiality of all program participants. PEACE program personnel must abide by PIPA 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 PEACE program services. Typically, these types of documents contain personal information. If intercepted, accessed or sent to the wrong address, a fax could put program participant's privacy and safety at risk.

The majority of the fax machines that PEACE programs use have the capacity to store information such as date and fax number of sent and received faxes. Larger machines have the ability to 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 and PIPA, PEACE program personnel will not include personally identifiable information of program participants to internal and external programs via fax without the signed informed consent of the program participant that has been documented in the PEACE program's *Release of Information* (ROI)[4] form. Before asking a program participant to sign the ROI, PEACE program personnel will inform the program participant of all risks associated with sending a fax containing personal information and their rights to revoke consent.

[4] Many PEACE forms mentioned throughout this guide can be found in the PEACE Program Toolkit at https://bcsth.ca/wp-content/uploads/2017/12/Peace-Program-Toolkit.pdf

PEACE program personnel will follow the recommendations for the faxing of personal information by the Office of the Privacy Commissioner of Canada https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/02_05_d_04/.

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

3.1 Sending of Personal Information

Procedures: Before agreeing to send a fax containing a program participant's personal information, PEACE program personnel will inform her or the mature minor 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 their private information and/or their location being compromised by **Agency XYZ's** fax number appearing on the received copy of the fax.

According to PIPA, women and mature minors must consent to having their information sent via fax. An *Informed Consent* form and **Agency XYZ**'**s** *Release of Information* form must be provided to program participants to complete and sign before faxing. Program participants will be informed that they can revoke their Release of Information at any time. This can be done via the PEACE program'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, PEACE program 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: PEACE program personnel at **Agency XYZ** will not require program participants to send personal information other than their name and contact number via fax (such as in *Referral* forms) in order to access services.

When a program participant is expecting PEACE program personnel to receive a fax containing personal information on their behalf, PEACE program 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, PEACE program 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 created date:
Policy review date:
Policy designate / overseen by:

4. Printer

Rationale: Printers are used to print documents which sometimes contain the personal information of women, children and youth accessing PEACE programs. Most printers have an internal hard drive which store 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 program participants could be breached. PEACE program personnel are committed to ensuring the privacy and safety of women, children and youth accessing their programs.

Policy Statement: PEACE program personnel at **Agency XYZ** will comply with PIPA when collecting, storing, using and disclosing the personal information of women, children and youth accessing PEACE programs.

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 **Agency XYZ** are destroyed before the machine is sold, donated or returned to the leasing company.

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

5. Scanner

Rationale: **Agency XYZ** is committed to protecting the privacy and confidentiality of all PEACE program participants. Most scanners have the ability to 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. PEACE program personnel must abide by PIPA 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 PIPA, PEACE program personnel at Agency 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 program participant's personal information, PEACE program personnel will inform her or the mature minor 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 **Agency XYZ** personnel, leasing companies or future owners of the machine.

According to PIPA, women and mature minors must consent to having their information collected. *Informed Consent* forms and the PEACE program'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. Women, children and youth will be informed that they can revoke the Release of Information at any time via the PEACE program's *Revocation of Information* form.

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

5.2 Storage

Procedures: Women and children asking PEACE program 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 machines capabilities.

Program participants will be made aware that copies of the scanned documents can automatically be downloaded and stored on **Agency XYZ's** computer network. If the agency'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: Agency XYZ's computer network is accessible by staff and third party vendors and sub-contractors. In compliance with PIPA, no documents containing personally identifying information will be kept on **Agency XYZ's** computer network. After scanning the document and giving a copy to the participant, PEACE program personnel will immediately delete all documents containing personal information from **Agency 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 **Agency 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 created date:
Policy review date:
Policy designate / overseen by:

6. Desktop Computers Owned by Agency

Rationale: Agency XYZ's PEACE program is committed to ensuring that all women, children and youth experiencing violence are able to communicate with PEACE program personnel using the most accessible method of communication for them, and that personnel have the necessary tools to provide PEACE program services.

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

Policy Statement: Agency XYZ provides computers for PEACE program personnel and for program participant use. Program participants will access devices, use logins, and Wi-Fi connections that are separate from PEACE program personnel.

6.1 Passwords

Procedures:

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

b) **Program participants:** 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, program participants will use a separate computer from program personnel that is participant designated. However, if there is not a computer for participants accessing the PEACE program, and the participant must use a computer designated for PEACE program personnel, PEACE program personnel will log off and the participant will log in using the Guest login and password provided. This will ensure the security of **Agency XYZ's** computer network and confidentiality and privacy of other participants.

6.2 Security Software

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

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

6.3 Computer for Program Participant Use

Procedures: The Administration Manager at **Agency 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 program participants are not connected to the agency's computer network and will consider disabling the ability to remote access into these computers and disable file sharing.

Program participants are encouraged to use their own USB drives to store documents rather than saving them on PEACE program 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 program participants to download and save important documents on. PEACE program personnel will also discuss the importance of password protecting USB drives with program participants.

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. PEACE program personnel at **Agency XYZ** and program participants will turn off the webcam when not in use. All **Agency XYZ's** computers will have a cover on their webcam (removable sticker, post it note, tape etc.) 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 agency or reveal the identity of program participants.

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 **Agency XYZ's** computers regularly.

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

7. Laptops Owned by the Agency

Rationale: Agency XYZ is committed to having safe and accessible technologies available for PEACE program personnel to provide PEACE program services. Laptops can make it easier for PEACE program personnel to do their work while working offsite. Laptops can help PEACE

program 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 PEACE program 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 PEACE program services. Someone with malicious intent and with access to a spyware program could quickly install it onto the device.

Agency XYZ's owned laptops have the ability to remotely connect to the agency'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 confidentially risks and potential for a data breach if the laptop is not secure.

Policy Statement: Agency XYZ permits the use of **Agency XYZ** owned laptops by PEACE program personnel while they are working offsite. Using laptops that are not owned by **Agency XYZ** are not permitted to be used for any work that includes the personal information of program participants. This can breach the confidentiality of women, children and youth accessing PEACE programs and put their privacy and safety at risk.

7.1 Passwords

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

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 programs) are downloaded on all **Agency XYZ** owned laptops and are regularly updated.

When needed, PEACE program 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 programs and software are up to date.

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

7.3 Accessing Wi-Fi

Procedures: PEACE program 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 centers, 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. PEACE program personnel at **Agency XYZ** will turn off the webcam when not in use. All **Agency XYZ's** laptops will have a cover on their webcam (removable sticker, post it note, tape etc.) 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 agency or reveal the identity of program participants.

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 **Agency XYZ's** computers regularly.

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

Procedures: PEACE program personnel will log into **Agency XYZ's** virtual network by using their unique User ID log in and password.

When using agency owned laptops in public spaces, PEACE program personnel will:

- position the laptop in such a way that confidential information cannot be breached (e.g. by others having the ability to read over their shoulder or from the next table). and,

- not access free public wireless connections when working on confidential program participant information.

7.6 Connection to Other Devices

Procedures: Many laptops have the capacity to sync with other devices such as MacBook's to iPads, iPhones and Apple watches. PEACE program personnel will ensure that their agency 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 (ex. Apple ID) for work laptops only and not use this ID with any other device.

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

8. Tablet Owned by the Agency

Rationale: Tablets can make it easier for PEACE program personnel to do their work while working offsite. Tablets can help PEACE program 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 **Agency XYZ** can breach the confidentiality of women, children and youth accessing the PEACE program 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 PEACE program.

Many tablets have the capacity to sync with other devices (e.g. iPads to iPhones, MacBook's and Apple watches). Tablets also allow users to download all kinds of applications (Apps). Some Apps give developers access to the tablet, including access to an individual's personal information, contacts, communication and photos. If PEACE program participant 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 use of non-Agency tablets will help to protect program participants, PEACE program personnel and **Agency 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: Agency XYZ allows the use of **Agency XYZ** owned tablets by PEACE program personnel while they are working offsite. In accordance with the guidelines provided by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for BC, using tablets not owned by **Agency XYZ** to communicate with program participants is prohibited.

8.1 Account Set Up

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

8.2 Passwords

Procedures: All **Agency XYZ** owned tablets are set up with a 4-6 digit security passcode by the Administration Manager and/or IT subcontractor. PEACE program personnel will receive the passcode when signing out the tablet. Each program 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: PEACE program personnel will not save or store any past or present PEACE program participant's contact information on **Agency XYZ** owned tablets.
Names of **Agency XYZ** personnel can be stored on the phones contact list on a first name basis only.

8.4 Personal Use

Procedures: When **Agency XYZ** loans a tablet to a PEACE program personnel to use for work purposes, **Agency XYZ** will communicate clearly all policies related to personal use of the agency tablet. These include policies related to:

- storage of personal contact information;
- taking personal photos or videos;
- downloading of Apps;
- connecting to other devices;
- location tracking/GPS enabling functions; and
- sending and receiving of personal communications.

8.5 Ownership and Privacy

Procedures: By law, **Agency XYZ** must ensure PEACE program personnel are following the policies outlined in this document and storing and destroying personal information in compliance with PIPA. If necessary, PEACE program personnel may be asked to provide their agency owned tablet to review security updates, and confirm that deletion of communications are up to date.

According to the OIPC BC, personal information in an organizations control may be subject to reasonable and acceptable corporate monitoring.

8.6 Sharing: Location and Content

Procedures: PEACE program personnel will ensure that location services are turned off on their agency tablet when they are not using it.

PEACE program personnel will also disable Bluetooth capabilities on their agency tablet to minimize the risk of interception.

Note: If the location settings are turned on and PEACE program 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: PEACE program personnel will not take photos of any woman or child accessing the PEACE program on **Agency XYZ** owned tablets without their informed consent. PEACE program personnel will only take work related photos and videos on their **Agency XYZ** owned tablets.

In compliance with PIPA, PEACE program personnel will inform program participants 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.
PEACE program personnel will obtain written consent on a P*hoto Consent* form from program participants before taking any photos. Participants 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 **Agency 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 **Agency XYZ's** main computer network and deleted off of the tablet within 3 business days.

8.9 Cloud Backup

Procedures: When setting up **Agency XYZ** owned tablets and the accounts associated with it, 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.

8.10 Connecting to Wi-Fi

Procedures: PEACE program personnel working on files and documents that contain any personal information or sensitive details or communicating via email or Instant Messenger with participants, 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: PEACE program personnel will ensure that their agency owned tablet is not linked to any other devices whether they are 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 programs) are downloaded on all **Agency XYZ** owned tablets and are regularly updated when new updates are available. If the tablets are being used offsite, PEACE program personnel will be asked to return the tablets to the Administration Manager 5 business days in advance of the IT subcontractor performing an update.

8.13 Downloading of Apps

Procedures: PEACE program personnel must be cautious of the types of Apps that are downloaded onto **Agency XYZ** tablets and fully read the Terms and Conditions of each App that they do download. PEACE program personnel will only download Apps that are necessary for their work. PEACE program personnel will pay close attention to what data these Apps are accessing and collecting by reading the permissions, either on the device or the App's website before downloading them to their work tablet.

If PEACE program 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. PEACE program personnel at **Agency XYZ** will download all available updates to their devices within 5 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 **Agency XYZ** owned tablet is stolen or misplaced. If the tablet is stolen or misplaced, PEACE program 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 program participants are on the tablet.

Policy created 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 **Agency XYZ** services. They help personnel to identify who is accessing services and ensure it is safe to answer the door.

Policy Statement: Agency XYZ has security cameras that are placed both indoor and outdoor and are used to monitor the common areas of the building the PEACE program is located in. In compliance with PIPA, PEACE program personnel will ensure that all potential participants of programs are informed of:

- security cameras are 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 is like any other personal data collected by agencies. In accordance with PIPA, **Agency XYZ** is required to receive informed consent when recording PEACE program participants. Therefore, before a woman or child receives services, personnel must inform participants:
   - that security cameras are on site
   - how long the recording is stored for, and
   - that with a subpoena, these recordings can be turned over to law enforcement.

   Security camera video recording disclaimers are included in Agency XYZ's *Informed Consent to Service* form and personnel must provide women, children and youth the opportunity to consent to recording.

b) **Personnel:** All PEACE program 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 **Agency 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 the personnel has chosen 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, women, children and youth who do not consent to be recorded.

d) **Notification and Signage:** To ensure transparency, visible notification through signs and information will be posted around **Agency XYZ** to inform women, children and youth accessing services that they are being recorded or viewed by cameras. Program 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 PIPA, **Agency XYZ** will only keep video recordings for the shortest time necessary to address safety and security issues, to a maximum of 1 year. The Executive Director, Administration Manager and IT subcontractor will determine the best way to store recordings and where.

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, **Agency 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."[6]

9.2 Cameras

Rationale: Like security cameras, cameras whether they use film, are digital or part of a mobile phone, store the personal information of personnel and women, children and youth participating in PEACE programs.

[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/

[6] 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/

Policy Statement: In compliance with PIPA, personnel, and women, children and youth accessing PEACE programs 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 PEACE program personnel. No photos will be taken of PEACE program personnel, or program participants without a signed copy of the *Photo Consent* form.

Procedures:

a) **Informed Consent of Personnel:** All PEACE program personnel at **Agency XYZ** will be informed by their supervisor at the time of their hiring that there may be opportunities, such as agency 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 has chosen to sign the *Photo Consent* form it will be filed in their personnel file.

b) **Informed Consent of PEACE Program Participants:** Before taking photos or videos of women, children and youth accessing the PEACE program at **Agency XYZ**, PEACE program personnel will ask participant 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, and
- inform participants of photo destruction policies.

Signed copies of program participant's *Photo Consent form* will be kept in their file.

c) **Storage of Photos and Videos:** Personnel taking photos or videos of **Agency XYZ** PEACE program personnel or participants will transfer the images from the camera, video camera or mobile device to the agency computer network within 3 business days. The photo/video will be deleted once transferred to the agency computer network or if it is determined not suitable for use.

If the photo(s)/video(s) are meant to be used at a later date, personnel will upload ONLY the photos and/or videos that will be used to the agency computer network within 3 business days. All other photos and videos will be permanently deleted off of 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 **Agency 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 agency 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: PEACE program personnel at **Agency XYZ** will not collect evidence (e.g. take photos of injuries). Alternatively, PEACE program personnel will educate PEACE program participants 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 PEACE program records are often subpoenaed, PEACE program personnel will not store any evidence for PEACE program participants. PEACE program personnel will educate PEACE program participants 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.

PEACE program personnel can link program participants to legal support or law enforcement if further help is needed.

f) **Recording a PEACE Program Session**

Procedures: PEACE program personnel will not tape or video record any participant sessions with PEACE program participants. According to PIPA, 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 created date:
Policy review date:
Policy designate / overseen by:

10. Electronic Databases

Rationale: Agency XYZ uses *(Agency XYZ to insert name of database)* database to electronically store the personal information of PEACE program participants. 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 program participants. Therefore, PEACE program personnel will only collect and store the minimal amount of personal information necessary to provide PEACE program services.

Policy Statement: Minimal and only essential information about PEACE program participants will be entered into **Agency XYZ's** electronic database. All PEACE program personnel will receive confidentiality and policy training about using **Agency XYZ's** database before entering personal information and case notes into the database.

10.1 User ID and Passwords

Procedures: Each PEACE program personnel will be given a unique USER ID and password to enable them to enter PEACE program participant's personal information and case notes into the database. This will help supervisors know who has accessed a program participant's file should there be a breach or privacy violation.

Only personnel who have reason to access the database for PEACE program reasons will be given a User ID and password. PEACE program employees will access the database to input PEACE participant information and case notes.

10.2 Database Access

Procedures: Each PEACE program personnel at **Agency XYZ** will access the database with their unique USER ID and password. PEACE program personnel will be assigned an access level which enables them to only access records of the program participants they are supporting. The database system is capable of tracking each participant record that a particular USER ID views, inputs, updates and changes. This will help maintain the privacy and confidentiality of program participants.

10.3 Security Software

Procedures: The Administration Manager and IT subcontractor will ensure that all computers that have the capacity to access **Agency XYZ's** database is protected with firewalls, anti-virus, anti-spyware and anti-malware programs. These programs will be updated once an update is available and will be completed within 5 business days of the new update.

10.4 Data Entry

Procedures: Agency XYZ's database is connected to the Internet. There is a potential for interception, a breach of data and/or a program participant's information being susceptible to a subpoena. Therefore, minimal participant information will be entered. This means that only information that is necessary to provide PEACE program service, 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, for example, "Session 1: focused on identifying feelings."

10.5 Subpoena of Data

Procedures: After receiving a subpoena for a PEACE program participant's record, PEACE program personnel will follow all steps outlined in **Agency XYZ's** electronic database policy manual. If it is determined that the PEACE program participant's record must be submitted, PEACE program personnel will inform their supervisor and work to only print off and submit the record asked for in the subpoena.

10.6 Destruction of Records

Procedures: In compliance with PIPA, **Agency XYZ's** Executive Director will work with the database developer to ensure the permanent deletion of records. For PEACE programs it is recommended that PEACE participant records be purged 7 years after the file is closed or 7 years after the minor has reached the age of maturity.

For more information about policies related to databases, please see BCSTH's "Privacy, Security and Confidentiality: Database Considerations for Violence against Women Programs" and BCSTH's Legal toolkit.

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

SECTION 2: ONLINE COMMUNICATION

1. Texting

Rationale: Texting can be a convenient way to communicate with PEACE program participants because it has become a primary mode of communication for many individuals, including for PEACE program participants who may be deaf or hard of hearing. However, because of the potential for mobile phones to be monitored (e.g. by parents of young people or by abusive (ex) partners) communicating via text can put participant's safety at risk. PEACE program personnel must consider the safety of participants before using text as a method of communication.

Policy Statement: Agency XYZ supports accessible communication between PEACE program personnel and (potential) PEACE program participants if it is safe to do so. PEACE program personnel will only text PEACE program participants (once consent has been given by the program participant) with **Agency XYZ** owned mobile phones *only*. PEACE program personnel who text with PEACE program participants on mobile devices owned by **Agency XYZ** will comply with the informed consent, storage and destruction of personal information policies that are in compliance with PIPA (See Policy 7: Mobile Phones Owned by Agency).

Because the definition of "record" is broad and can include all telecommunication with participants (texts, emails, instant messages etc.), **Agency 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 PEACE Program Colleagues

Procedures: PEACE program personnel communicating via text with other **Agency XYZ** personnel using agency owned mobile devices will not text any personally identifying information about a program participant.

PEACE program personnel will not store the full name of **Agency XYZ** personnel in the contacts of their mobile device.

1.2 Texting PEACE Program Participants

Procedures: Before communicating via text with PEACE program participants, PEACE program personnel at **Agency XYZ** must discuss with participants about their preferred methods of communication and discuss any risks to privacy and safety. Program

participants should be informed that if the perpetrator or parent 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 (i.e. instant messaging) will be discussed prior to texting. PEACE program personnel will inform participants that texting will be used only for general purposes such as appointment reminders, and not for counselling.

PEACE program personnel will also inform program participants:

- the office hours that they, and other, program personnel are available;
- that their text will be returned within 2-3 business days as personnel is not available 24/7;
- alternative people to talk when PEACE program personnel are not available;
- what can and can't be discussed via text; and
- safety code words.

Once participants are informed of any risks, it is up to them if texting with PEACE program personnel is a safe option.

PEACE program personnel will receive written, time limited, informed consent from a program participant before texting by asking the program participant to consent to **Agency XYZ's** *Consent to Communicate via Technology* form.

PEACE program personnel will only text general information with program participants. No personal information or communication that could be harmful to a participant will be discussed. PEACE program 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 participant's record and contents of the text must be included in a subpoena.

1.3 Deleting Text Logs

Procedures: PEACE program personnel with an agency 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, voicemail from a potential or existing program participant 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 participant's record has been received.

1.4 Storing PEACE Program Participant Contact Information

Procedures: PEACE program personnel will not store PEACE program participant's contact information into their agency owned mobile device. This 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 PEACE program participants via text, PEACE program personnel at **Agency XYZ** will safety plan with the participant 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 program participant's phone will see the mobile phone number that PEACE program personnel is texting from. PEACE program 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 PEACE program participant especially if they are living in the same household, share guardianship of the participant or if the perpetrator is the owner of the phone and has access to the account. PEACE program personnel can suggest that they share a code word or code name with the program participant that the participant has to answer before continuing a conversation with them.

c) **Storing PEACE Program Personnel Information:** PEACE program personnel can suggest that the program participant not store their contact number, including their name and mobile phone number, in the participant's contacts. Program personnel can suggest a general alternative name or business to store the PEACE counsellor's phone number under so that she may not be questioned if the perpetrator is monitoring her phone.

d) **Boundaries:** PEACE program personnel will recommend an alternative number for the program participant to call or text after hours, such as a 24 hour crisis line or 9-1-1.

PEACE program personnel will be transparent in letting participants know that they are unavailable after their work day and that they may not respond for 2-3 business days.

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

2. Email

Rationale: Many PEACE program personnel use email daily in their work to communicate with women and young people directly or to coordinate services with other community programs. Email however is not the safest way to communicate. Emails can be forwarded accidently or intercepted by someone for whom the email was not intended.

Policy Statement: Agency XYZ is committed to communicating with women, children and youth in the most accessible and safest way possible. For some program participants, 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 program participants (texts, emails, instant messages etc.) **Agency XYZ** requires all PEACE program 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 participants on all devices.

2.1 Assessing Women's Safety before Emailing

Procedures: PEACE program personnel will follow email best practice and assess any potential safety risks before emailing or replying to an email from a PEACE program participant.

a) PEACE program personnel will only communicate with (potential) program participants using an **AGENCY XYZ** email address. PEACE program personnel will not use their personal email to communicate with PEACE program participants.
b) PEACE program personnel will confirm with PEACE program participants if it is safe to email them. This will include, but is not limited to, asking:
   - If the perpetrator has access to their email and knows their password?

- Is the device that she checks her email on connected to another account or device? For example, 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 program participant has answered yes to any of the above questions, suggest that the program participant:

- 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 PEACE program personnel know that she is not being impersonated by her perpetrator or anyone else.
- Discuss email safety and privacy with program participants, 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) PEACE program personnel will not store a participant's email address in their personal and/or agency email address book or mobile device contacts.

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

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

f) Program personnel will delete any emails from program participants once they are 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 program.

2.2 Responding to PEACE Program Participant Emails

Procedures: PEACE program personnel will always delete the previous conversation thread when responding to emails from program participants. 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.
PEACE program personnel will also:

- ensure that the subject line in the email is something general
- only communicate with participants using their **Agency XYZ** email address, and
- refrain from sending emails to participants from a PEACE program personnel's personal email address.

2.3 Deleting Emails from an Inbox and Delete Folder

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

2.4 Accessing Email Remotely

Procedures: PEACE program 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 outlining monitoring practices. In accordance with the Office of the Information and Privacy Commissioner of BC the following procedures will take place before accessing email remotely.

a) Approval from a supervisor or Executive Director is needed in order to be able to access emails remotely. Approval will largely depend on whether this capability is needed in order for PEACE program 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;
- If the mobile device being used is an agency owned device;
- If the device is not an agency owned device:
  - Who has access to the mobile device?
  - Is the mobile device password protected?
  - Are any accounts such as an Apple 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 (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 (location) settings turned off when not in use.

d) PEACE program personnel will know which Apps have the ability to access all information from their phone, including from their work email.

2.5 Corporate Monitoring of Devices

Procedures: In accordance with the Office of the Information and Privacy Commissioner of BC, PEACE program personnel wishing to communicate with program participants via online communication (such as access email remotely, texting and instant messaging) must understand that if there are any concerns by their supervisor or Executive Director over one's online communication, **Agency XYZ** personnel are subject to reasonable and acceptable monitoring of the device (either **Agency XYZ** owned **or a personal device)** used to access email remotely. Personnel wishing to access their email remotely will be given a *User Agreement* form outlining monitoring practices. Personnel will refer to **Agency XYZ's** Operational Policy for more information.

2.6 Email Back up to Third Party Cloud

Procedures: In accordance with the Office of the Information and Privacy Commissioner of BC, the Administration Manager or IT subcontractor will check regularly to ensure that their **Agency XYZ** email is not being automatically backed up to a third party cloud server other than the one that is set up by **Agency XYZ.** If PEACE program 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 Participants:

Procedure: Internal communication via email about participants is restricted. PEACE program personnel will not include names of participants or other identifying information in emails.

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

3. Social Media

Rationale: Agency XYZ uses Social Media platforms such as (*Agency XYZ to insert)* 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 programs struggle. It is important to have a policy beforehand so PEACE program personnel can address it with confidence and clarity. Having a clear purpose for why **Agency XYZ** uses social media will help the agency develop policies around responding to opposing or negative views.

Policy Statement: PEACE program personnel will never post participant information or non-public domestic violence or sexual violence accounts on **Agency XYZ** social media accounts as this may reveal the identity of women, children and youth accessing services and violate her/his confidentiality.

3.1 Access to Agency Social Media Accounts

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

Agency XYZ's PEACE program personnel are welcome to "follow" or "friend" or "like" **Agency 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 (Past) Participants

Procedures: PEACE program personnel will never post the personal information, including photos, videos, and concerns about past and present program participants on their personal or **Agency XYZ** social media pages. This also includes, but is not limited to, commenting on PEACE program participant's posts that could indicate that they are past or present participant of **Agency XYZ** services.

3.3 Posting about Agency XYZ Personnel

Procedures: PEACE program personnel will always receive informed consent from Board members, employees, sub-contractors, service providers, volunteers, trainees, work placement and student interns before posting pictures, images, and names on social media. The administrators of **Agency XYZ's** social media accounts (See Section 13.1) 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 Program Participants Communicating via Social Media

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

- To contact **Agency 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 agency or another organization.
- That **Agency 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 agency 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 (texts, emails, instant messages etc.) that the conversation happening online can be used if her records are 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 program participant.

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

3.5 What to Post on Agency XYZ Social Media Accounts

Procedures: Only social media account administrators will post on **Agency 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 is a reflection of **Agency XYZ**.
- What they post should support **Agency XYZ's** communication goals. (e.g. if the social media pages are a way to showcase **Agency XYZ** and its activities their policy may say that they only post activities that **Agency XYZ** supports or is involved in. If **Agency 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 Agency XYZ's Social Media Account

Procedures: Only social media account administrators will respond to posts on **Agency XYZ's** social media accounts. Social media account administrators will make a decision about if and how they will respond to opposing views and ensure that their response reflects **Agency 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 Agency XYZ's Social Media Account

Procedures: Agency 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 **Agency XYZ** shares through its social network and whether it is appropriate to share that with the person who wants to join the agency network. If **Agency XYZ** uses social media to raise awareness and therefore wants to accept all "friend" or "follow" requests, it is important that the agency 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 Agency XYZ Social Media Account

Procedures: Only social media account administrators will respond to or delete posts on **Agency XYZ's** social media accounts. **Agency 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 **Agency XYZ's** content guidelines.

3.9 Social Media Monitoring and Oversight

Procedures: Agency 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 **Agency 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, **Agency 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:

- Use of personal social media during work

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

4. Video Chat

Rationale: Video chat can be a convenient way to communicate with PEACE program participants, if it is safe to do so.

Policy Statement: PEACE program personnel at **Agency XYZ** who have received a request from participants 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 **Agency XYZ** and has IT security up to date. PEACE program personnel will only use agency accounts. If the supervisor is unsure if the technology is in compliance with PIPA, they will request support from the IT subcontractor.

4.1 Assessing Risk

Procedures: Before asking for permission to begin service delivery via video chat with a woman, child or youth accessing the PEACE program at **Agency XYZ**, PEACE personnel must assess for safety risks associated with using video chat.

Personnel will begin assessing risk by asking the program participant:

- What device they plan to use to video chat?
- If the device has an up to date anti-virus program running?
- If the perpetrator has access to the device?
- If the perpetrator is tech savvy?
- If she has reason to believe that her device is being monitored and explain the potential risks to her safety?
- If the video chat account is used by more than one person?
- If the device the video chat will be taking place on will be used by more than one person?
- If the account is accessible to or connected to other devices?
- If the video chat account is password protected?
- If the perpetrator has access to the video chat account?
- If the perpetrator lives at the home where the program participant will be chatting?

If the program participant answers yes to any of the above questions discuss with a supervisor if it is safe to communicate with this program participant online. 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, PEACE program personnel at **Agency XYZ** must safety plan with the participant before communicating via video chat.

Safety planning with the program participant will include:

- Advising the program participant to not save **Agency XYZ's** contact information on the device or in the chat program.
- Ensuring that the device is used in a private location.
- Creating a plan or code word that the program participant will use if the chat is interrupted or disconnected.
- Informing the program participant that PEACE program personnel cannot participate in video chat if she wishes to record the chat.

Prior to beginning a video chat, PEACE program personnel will inform participants of any potential risks and get the participant's informed consent to provide service via video chat through the appropriate *Informed Consent* form.

4.3 PEACE Program Personnel Video Chat

Procedures: PEACE program personnel at **Agency XYZ** requesting to video chat with participants will ensure that:

- The device they will be using is an agency owned device.
- The device has the most up to date anti-virus software.
- The video chat will only take place at an agency site, in an office with a door and in a location that will not capture any other program participants accessing **Agency XYZ** services.
- They will use a video chat account set up with their agency work email.
- They will not save the participants user name 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 created date:
Policy review date:
Policy designate / overseen by:

SECTION 3: AGENCY TECHNOLOGY

1. Website Safety

Rationale: Agency XYZ has a website to share information about services and to raise awareness about agency programs available to support women, children and youth experiencing violence.

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

1.1 Safety Alert

Procedures: Many perpetrators monitor survivors' online activities, whether through looking over their shoulder, manually going through the Internet browsing history, or via computer or mobile phone monitoring software. **Agency XYZ's** Executive Director, Administration Manager and IT subcontractors will ensure that a safety alert is always on the agency's website to remind visitors that their activities could be monitored or viewed by someone who has access to the device. PEACE program counsellors will advise participants of these safety features.

1.2 Quick Escape Button

Procedures: Agency XYZ commits to having a quick escape button on its website where 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. PEACE program personnel will advise participants of these safety features and their limitations.

1.3 Web Form

Procedures: Some women, children and youth experiencing violence will want to email the PEACE program to ask for help or resources and will go to **Agency 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, **Agency XYZ** will use a web form where visitors can send personnel their message. This message will be submitted as an email to the PEACE program personnel.

PEACE program personnel will advise participants 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 Program Participants Online

Procedures: Agency XYZ commits to never posting any information, photos, or videos of women, children and youth accessing PEACE program services on the agency website; except when informed consent has been given.

1.5 Posting of Agency Personnel

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

1.6 Accurate Information

Procedures: Agency XYZ commits to posting only accurate information on the agency website. **Agency XYZ** will include information specific to service delivery, service delivery area and ensure any links to resources or community partners are up to date and accurate. PEACE program personnel will advise participants of these resources.

1.7 Accessibility

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

Agency XYZ will:

- Check that images on the agency website have alternative text descriptions (html alt text).
- Ensure 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 agency 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 created date:
Policy review date:
Policy designate / overseen by:

2. Internet Use

Rationale: Having the Internet available gives PEACE program personnel at **Agency XYZ** a tool to help provide PEACE program services and empower program participants to make steps towards living safely and independently from violence.

Procedures: Agency XYZ will provide PEACE program personnel with the tools necessary to provide PEACE program services. This includes providing safe and secure access the Internet.

2.1 Acceptable Use

Procedures: Program participants will access the Internet by logging on to **Agency XYZ** computers using Guest login and passwords. Guest login and passwords will be provided by PEACE program personnel.

If it comes to the attention of PEACE program personnel that program participants are accessing problematic sites, this will be reported to their supervisor. The supervisor will communicate with the Executive Director who will make a decision on whether the IT subcontractor should block certain content.

The Executive Director will work with the IT Subcontractor to increase the privacy of participants 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; and
    - disabling auto-save logins and passwords.

Because program participants are accessing a shared computer, PEACE program personnel will:

- Suggest that program participant's 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 **Agency XYZ's** IT subcontractor.

2.2 Personal Use

Procedures: PEACE program personnel while at work at **Agency XYZ** can access the Internet for acceptable use during personal time.

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 and the Information and Privacy Commissioner for BC suggest that agency owned mobile devices (mobile phones, tablets and laptops) are the only mobile devices to be used by PEACE program personnel when communicating with women, children and youth accessing PEACE program services.

Policy Statement: As per recommendations from the Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioner for BC, only agency owned mobile devices are to be used when communicating with women, children and youth. **Agency XYZ** is responsible for paying the monthly and/or annual plan of the device and negotiate all contracts associated with the device.

Procedures:

a) **Agency XYZ** is responsible for the purchase and payment of agency owned mobile devices. **Agency 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 PEACE program supervisor. If these charges are due to personal use, it is the sole responsibility of

the PEACE program personnel who has been granted use of the mobile device while employed at **Agency XYZ** to reimburse the agency for these charges**.** **Agency XYZ** will negotiate all terms and contracts for the mobile device.

b) **Supplementation of Personnel Devices: Agency XYZ** will not supplement the monthly fees of non-agency owned phones.

SECTION 4: TECHNOLOGY SECURITY

1. Wi-Fi

Rationale: Wi-Fi connectivity can make connecting to the Internet at **Agency XYZ** more accessible for PEACE program personnel and the women, children and youth who access our services. Providing access to the Internet via Wi-Fi can be helpful for PEACE program personnel to carry out their work on agency owned mobile devices. Having Wi-Fi accessible to women, children and youth accessing PEACE programs can be empowering as participants 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: Agency XYZ PEACE program sites have Wi-Fi capacity. Because of the sensitive nature of the work done by PEACE program personnel, access to **Agency XYZ** Wi-Fi by personnel and program 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 **Agency XYZ's** PEACE program site's Wi-Fi is as secure as possible. The proper configurations will be in place to make sure that the PEACE program 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 a PEACE program 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: PEACE program 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 **Agency XYZ** personnel use only. A second guest Wi-Fi network will be set up

and available to PEACE program participants in need of accessing the Internet. PEACE program personnel will give out the password to the Guest Wi-Fi network to participants at their discretion.

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

(Agency XYZ insert name of Wi-Fi network) is a Guest Wi-Fi Network for PEACE program participants and **Agency XYZ** guests to log in to while they are on site.

1.3 Password Protection

Procedures: There are two Wi-Fi networks at **Agency XYZ**. One for PEACE program personnel and one for program participants. 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 PEACE program personnel when needed. Because of the sensitive nature of PEACE program work, PEACE program personnel will not access the Internet through the guest Wi-Fi network.

PEACE program 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 PEACE program personnel need to access Wi-Fi offsite for **Agency XYZ** related work, PEACE program 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 program participants, they will not connect to free public Wi-Fi.

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

SECTION 5: ADDITIONAL CONSIDERATIONS

1. Information Technology Support

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

Policy Statement: Agency XYZ is committed to ensuring that it's IT is as safe and up to date as possible and will subcontract xxx to do this. The Administration Manager and Executive Director will review the satisfaction of IT services annually.

1.1 IT Support

Procedures: When PEACE program personnel at **Agency XYZ** are in need of 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 a PEACE program personnel at **Agency XYZ** has 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 created date:
Policy review date:
Policy designate / overseen by:

2. Accessibility

2.1 Using Technology to be More Accessible with Program Participants

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

Policy Statement: **Agency XYZ** recognizes that under the Canadian Human Rights Act, it is against the law to discriminate on the basis of race, colour, age, national or ethnic origin, religion, marital status, family status, disability, sexual orientation, sex, pregnancy, child-birth and a pardoned criminal conviction. As such, **Agency XYZ** and its PEACE programs ensures that IT services and programs are accessible to women, children and youth. **Agency XYZ** will not practice or engage in unlawful discrimination on the basis of 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. **Agency XYZ** will provide PEACE program services that are sensitive, responsive and accessible to the diverse needs of the women, children and youth it serves and promote cross-cultural understanding, safety and respect for diversity among participants and staff.

Procedures: During intake, PEACE program personnel at **Agency XYZ** will assess if a program participant is in need of extra support in order to participate in PEACE program counselling. If it is determined that one of the needs is to communicate through the use of technology, PEACE program personnel will consult with their supervisor to explore the best way to obtain assistive technology or translation services to reduce barriers for PEACE program services.

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

3. Purchasing

Rationale: It is important for PEACE program personnel to have access to the appropriate technology tools needed to support program participants.

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

3.1 New Software Requests

Procedures: When the budget allows, **Agency XYZ** may purchase new software to enhance PEACE program services provided to program participants.

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

3.2 New Hardware Requests

Procedures: When the budget allows, **Agency XYZ** may purchase new hardware devices to enhance the PEACE program services provided to program participants.

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

3.3 Applications for Mobile Devices

Procedures: PEACE program personnel at **Agency XYZ** may find that there are Apps available to purchase through App stores that will enhance the services provided to women, children and youth accessing the PEACE program.

PEACE program personnel wanting to purchase an App must do their due diligence and read the terms and conditions to ensure that the App:

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

A request to purchase the App must be made to the program 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 created date:
Policy review date:
Policy designate / overseen by:

4. Monitoring of Technology

4.1 Right to Monitor Technology

Rationale: Agency XYZ is transparent about its legal rights to monitor the technology used to provide service to participants of the PEACE program.

Policy Statement: Agency XYZ is within its legal rights to monitor the technology used for PEACE program services that collects personal information of participants (e.g. text, email, etc.). According to the Privacy Commissioner of Canada, this includes a PEACE program personnel's personal device. Though **Agency XYZ** does not monitor the technology of personnel, PEACE program personnel should be aware that if a targeted investigation where there are reasonable grounds for suspicion or wrongdoing, and only when other less privacy-intrusive measures have been exhausted, **Agency XYZ** is within its rights to "reasonable and acceptable corporate monitoring"[7] of a personal and agency owned device.

Procedures: When it has been deemed necessary to monitor agency owned technology, **Agency XYZ** will define clear guidelines related to process, including how much time a program 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 created date:
Policy review date:
Policy designate / overseen by:

5. Reporting Misuse

Rationale: Agency XYZ is committed to safe technology use and using technology in compliance with PIPA and the Charter of Human Rights to preserve the privacy, confidentiality and safety of women, children and youth accessing the PEACE program.

[7] https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_byod_201508/

Policy Statement: There may be times when PEACE program personnel at **Agency XYZ** suspect that agency owned technology or systems are being misused by agency personnel or program participants. In a case where misuse of technology is suspected the following processes will be followed.

5.1 Reporting Process

Procedures: If PEACE program personnel suspect that agency owned technology or systems are being misused by agency personnel or program participants, PEACE program personnel will notify their supervisor, Administration Manager or Executive Director.

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

6. Using a Personal Device for PEACE Program Services

Rationale: While using a personal device owned by PEACE program personnel may be more convenient or cost effective, the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Officer of BC strongly recommend 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 PEACE program personnel personal mobile device. This is to ensure that the personnel of the organization comply with PIPA.

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

- when communicating with PEACE program participants.
- for the collecting the personal information of program participants.

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

Procedures: Agency XYZ will create a User Responsibilities document that outlines:

- Acceptable and unacceptable uses of the BYOD and the collection of personal information of PEACE program participants.
- Employee functions and roles that are appropriate candidates for a BYOD program.
- 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.
- 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 PIPA on the personal mobile device for all staff using their own device.

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. "Agency's Use of Technology Best Practices & Policies Toolkit." https://www.techsafety.org/resources-agencyuse Retrieved February 7, 2018.
- Office of the Privacy Commissioner of Canada. "Contemplating a Bring Your Own Device (BYOD) program?" 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) Program 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 programs." https://endvaw.ca/wp-content/uploads/2016/05/Guide-to-Policy-Development-for-Feminist-Anti-Violence-Programs-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.