Technological Communication Policies & Procedures

FOR THE "USING TECHNOLOGY TO BETTER SUPPORT SURVIVORS: INNOVATION IN FRONTLINE SETTINGS" PROJECT

Pamela Cross

OCRCC TECHNOLOGICAL COMMUNICATION POLICIES AND PROCEDURES

General comments:

1. Yellow highlighting indicates you need to insert information specific to your Centre. There are many places where you need or may want to do this – I have just highlighted the major spots.
2. I have used plural pronouns rather than singular to reflect a trans-inclusive approach, but of course you can change this to the female singular if that reflects your agency's philosophy.
3. I have used the terms client and woman interchangeably because I don't know what language each of your Centres uses.
4. Because I don't know what your present policies and procedures are, you may not need all of what follows. In other cases, you may want to simply cut and paste a few words or phrases from what I have developed into your existing policies and procedures.
5. You should review your present policy and procedure manual to ensure that you update as needed to reflect your Centre's use of technology.
6. I have provided a few general policies and procedures relating to confidentiality and recordkeeping just in case they are helpful.
7. Whatever you do in terms of policy and procedure development, you should plan for staff training over the next year to make sure everyone is up to speed with your Centre's framework for using technology for the delivery of services. The training should include not just the policies and procedures but operational protocols and skills development such as, in particular, counselling and communication techniques to assist in:

- establishing and maintaining appropriate boundaries between counsellors and women
- dealing with situations where a woman stops responding in an online conversation
- responding to complex emotions that may arise during an online conversation
- handling an online disclosure that indicates the woman is in immediate danger
- ending an online conversation appropriately

8. I feel very strongly that staff should not be using their personal devices to communicate with clients. I have a number of reasons for this, including staff safety and privacy, client safety and privacy, challenges setting and maintaining appropriate work/personal boundaries for staff and accessibility issues for staff who choose not to or cannot afford to have electronic devices. I have developed a number of policies and procedures to support Centres where staff use their own devices, but please know that this is not what I think is best. These policies can be adapted for situations where devices are owned by the Centre, because the principles remain the same.

9. If your staff are required to use their personal devices for work, this requirement should appear in any job postings and all position descriptions.

Human Resources

1. Use of personal devices

Policy: Whenever possible, X will provide its staff and volunteers with work-owned electronic devices, including smart phones, tablets and laptop computers.

When this is not possible, staff will be expected to use their personal devices in a professional manner that ensures the highest possible level of safety and privacy for the women they support and themselves.

Procedures:
All electronic devices used in the course of the Centre's work, whether owned by the Centre or by the staff person, shall be password protected.

A record of current passwords shall be maintained by (XXX insert name of staff person with this responsibility) in a confidential and secure location.

Staff shall change the password on their personal devices used for Centre work every three (3) months, and shall provide this information to XXX. XXX shall change the password on centre-owned electronic devices every three (3) months and shall update the list of current passwords accordingly.

XXX shall decide on the appropriate format for passwords (eg. minimum number of characters, combination of upper and lower case, numbers, letters, symbols etc.)

Staff shall provide XXX with identifying information about any personal devices they use for Centre work.

If staff use personal devices for Centre work, they shall be required to transfer any client-related information to a Centre device or to take screen shots of that information and send it to a Centre device as required under the circumstances, but at a minimum once a month.

When a staff member leaves the employment of the Centre, she shall transfer all client-related information to the Centre as noted above and scrub her device of such information. The Executive Director or her designate may inspect the device to ensure this has happened.

If a staff member fails to scrub her device for any reason, the Centre shall use the appropriate software to do a remote wipe of her device(s).

Staff using personal devices for Centre work are required to keep work and personal files and information separate on those devices and to have different passwords to access work and personal files.

Staff using personal devices for Centre work may only install apps as permitted by the Centre. The Centre's decisions about permissible apps will be made based on privacy, confidentiality and safety concerns for both staff and clients.

Whether a device is owned by a staff person or by the Centre, if it goes missing for any reason, this shall be reported to XXX, who shall immediately contact the provider to try to track the device and to lock it from use by anyone who may have it.

2. Data usage reimbursement

Policy:
X shall reimburse staff for their data usage charges when staff are required to use their personal electronic devices for Centre work.

Procedure:
XXX shall determine the portion of the staff person's data usage charges to be covered by the Centre based on how much Centre work each staff person does using their personal device.

This cost shall be evaluated and adjusted on an annual basis as may be needed to reflect changes in the charge and/or changes in the staff person's use of their personal device for Centre work.

Reimbursement will be paid (annually, monthly, on the staff person's anniversary, etc. – you pick) by (cheque, automatic deposit, etc.).

3. Staff privacy and safety

Policy:
The Centre takes the privacy and safety of its staff very seriously, including with respect to the use of technological communication in the course of work responsibilities.

Staff are expected to consider their safety and privacy in their use of technological communication in the course of their work.

Procedure:
The GPS function on electronic devises shall be decommissioned, whether on Centre-owned or personally owned devices, unless to do so would create a greater safety risk.

No device shall show the identification of the caller.

Staff are expected to keep the device – whether their own or Centre-owned – either with them or in a secure location at all times.

It is the responsibility of the Centre to ensure staff have access to regular training on issues relating to online safety.

4. Boundary setting

Policy:
The Centre acknowledges that boundary issues will arise when staff use their personal devices for work-related responsibilities and is committed to supporting staff to set and maintain appropriate and professional boundaries with all clients.

Procedure:
Client access to counsellors via technological communication will be set out in the informed consent document, which will be reviewed by the counsellor and client before the client signs it.

Staff will not provide their personal contact information to clients under any circumstances.

Except in extraordinary circumstances, which must be approved in advance by the Executive Director or her designate, staff will not have contact with clients outside the staff person's regular hours of work.

Counsellors are expected to communicate their availability to clients in a clear and positive way, reinforcing this from time to time as may be needed.

Operations policies and procedures

1. Principles to guide the work

Policy
X keeps records and files about the women it serves and the services they and their dependents receive. X believes that keeping records is one component of providing all women and their dependents with consistent, high-quality services and is consistent with the Centre's feminist principles.

The Centre also recognizes that the creation of records creates an inherent power imbalance between those who create the records and those about whom the records are created. Its policies, procedures and practices related to recordkeeping are intended to make the process as transparent and accessible as possible.

Procedure
Good records:

- help provide stability and predictability
- promote effective communication among staff
- support staff in providing information on behalf of women
- promote staff and agency accountability and professionalism
- help to ensure that all women using services are treated in a fair and consistent manner
- allow women to have information about themselves
- document consent for services provided
- document that the limitations to confidentiality have been explained adequately
- enhance safety for women and staff
- support the development and implementation of women's safety plans
- provide protection for staff, volunteers and the Centre if questions arise about the quality of service or ethics of staff or the Centre
- promote efficient collection of information and data
- satisfy funder requirements

The following definitions apply to all recordkeeping and confidentiality-related policies and procedures.

Records: are the documents created by Centre staff/volunteers relating to women and their dependents, including but not necessarily limited to, forms signed by women, the general assessment form, the intake form, data sheet, child abuse report documentation form, safety plan agreement, homicidal risk documentation information form and suicide risk documentation information form.

File: is the collection of a woman's records.

Records will include only the information needed to support effective service delivery to the woman and to ensure the safety of the woman, other women receiving services and staff/volunteers.

2. Confidentiality and Privacy

Policy:
X understands the importance of providing confidentiality to and protecting the privacy of the women using its services and their dependents. The Centre is committed to respecting the privacy of women and their dependents to the limit allowed by the law. This commitment is compatible with the Centre's belief that women have the right to make independent choices about their lives and that those choices must be respected.

While X is committed to working collaboratively with other agencies and professionals, its commitment to the safety and privacy of the women using its services and their dependents is its top priority.

The Centre uses technological communication in its work – both internally and in the provision of services – and its commitment to women's privacy and confidentially extends to such situations. Any and all policies and procedures related to confidentiality and recordkeeping are intended to cover the use of technology in the delivery of services.

The Centre expects Board, management and frontline staff, volunteers, visitors and student placements to keep all information they receive through their connection with X in the strictest confidence. Every individual associated with X in one of these capacities must sign a confidentiality commitment.

All those receiving services from or participating in programs run by the Centre are also expected to keep information they receive in this context in the strictest confidence. Women must sign a confidentiality commitment as part of their initial interview or intake, which is then kept in their file.

Procedure
Confidentiality: is the obligation of the Centre and its staff/volunteers not to *willingly* disclose information obtained in confidence from someone without that person's consent, unless required by law to do so.

Privacy**:** is the right of individuals to determine when, how and to what extent they share their personal information.

Personal Information**:** is any information that can be used to distinguish, identify or contact a specific individual. This information can include any individual's opinions or beliefs as well as facts about or related to the individual.

X collects and uses personal information only to support the services it provides to women. All such information is kept in confidence. Staff are authorized to access this

information only on a need to know basis for the purpose of providing services to women.

Women provide consent for the collection and use of their personal information.

X will disclose personal information under some circumstances:

i. when required by law, in particular, by an order of either the family or criminal court (for example, a subpoena or application for production of records) or when required by child protection legislation (for example, as required by duty to report legislation);
ii. when the person to whom the information relates is a danger to herself or others
iii. when the person to whom the information pertains has provided a properly written and signed Consent to Release form

Non-compliance with this policy will be taken very seriously. In the case of a staff member, the Centre discipline policy will be used. Women who share confidential information with the intent to cause harm may have services terminated immediately.

3. Use of technological communication

Policy:
The Centre acknowledges that the appropriate use of technological communication can provide an effective and cost-efficient form of professional communication both internally and externally.

Staff are expected to use such technology in a professional and respectful manner at all times.

Procedure:
All technological communication tools will be used in a manner that is consistent with the Centre's mission/vision/philosophy and that follows all relevant Canadian and Ontario laws, including criminal and copyright law.

Technological communication will be treated with the same level of formality as other forms of communication. Nothing will be said that would not be said in any other form of business communication/correspondence.

Email communication will become part of a client file following the same process as any other form of communication.

If electronic communication is used with respect to a client for any reason, every effort will be made to ensure the client's confidentiality is maintained.

Email communication between staff and clients will be limited to sharing information that could not compromise the safety or privacy of the client or the staff person.

Staff and volunteers will send and receive personal communication in a way that does not interfere with their professional responsibilities or with the needs of clients.

When selecting web-based platforms and apps. to be used for service delivery with clients, the Centre will consider:

- Level of privacy offered
- Whether or not the company is subject to American anti-terrorism legislation with respect to the capture and storage of information
- The company's policies and procedures related to capturing and storing information and to providing that information to other third parties, with or without the consent of the Centre, the client or any other person whose information may be shared
- Willingness of the company to respect the unique issues presented by providing services to survivors of sexual violence using technological communication
- Any other factors that may be necessary

4. Providing services using technological communication

Policy:
X understands the importance of providing services in a number of formats in order to accommodate a diversity of needs among the women who use the Centre's services. While in-person services continue to be the Centre's focus, services are also provided electronically.

All decisions made by the Centre about how to deliver services to women using technological communication shall be made using a woman-centred, trauma-informed, harm-reduction framework that places the safety and privacy of women at the centre.

Women will not be required to receive service using technological communication if they do not indicate they wish to by completing and signing the relevant informed consent form.

Procedure:
Electronic formats by which services may be delivered include but are not limited to: email, text message . . . (list whatever your Centre is doing in here.)

Services that may be provided using electronic communication include:

- setting and confirming appointments with clients
- crisis counselling
- list whatever else you do technologically

In addition, staff communicate with one another and with volunteers by email and text as follows:
Insert whatever your centre does in this area

5. Centre use of social media

Policy:
The Centre uses social media in combination with other forms of communication, including email, faxing, postering, print media, etc. for the purposes of communicating with the public to ensure its outreach is as broad as possible.

Social media will not be used to communicate directly with individual clients, because of the lack of privacy it affords.

Procedure:
The Centre will use social media as appropriate to promote such things as:

- Fundraising activities
- Events such as an open house or the Centre's Annual General Meeting
- Calls for nominations to the Board of Directors
- The Centre's Annual Report
- Employment opportunities

Use of social media will be the responsibility of XXX, who will ensure all social media content is developed in a professional manner.

6. File Ownership

Policy Statement
Client files in any form including electronic are the property of X, which is responsible for their maintenance and management.

The following are not considered part of the client file and so are not the property of the agency:

- materials such as diaries and artwork produced by the client
- materials such as medical records created by third parties
- written statements made to the police
- legal documents shared by women with Centre staff/volunteers

Any artwork by clients that is donated to the agency becomes the agency's property. The agency and the woman will determine together what type of public recognition, if any, the woman is to receive for her donation.

Procedure:
Women will be informed when their file is opened that the file is owned by X and not by them. Women will also be told about the process they may use to access their file.

Staff will explain to women why they are collecting the information and the purposes of the record that is being created.

At the time the file is opened, staff will explain the agency's confidentiality and privacy policy and procedures, including the limitations to confidentiality, to the woman and will provide her with a written handout summarizing this information. This will be reinforced with the woman throughout her relationship with the agency.

The woman will be required to sign an acknowledgement that the confidentiality policy and procedures, including limitations, have been explained to her.

Recordkeeping information, including any forms women must sign, will be made available in plain language, in multiple languages and in accessible formats, as needed.

7. Client Access to Files

Policy Statement
X's feminist approach to recordkeeping allows women to have reasonable access to their own files so they can have information about themselves and the work they are doing with the agency.

Procedure
Women may have access to their files by making a verbal request to staff, who will respond in a timely manner.

If there is any uncertainty as to the woman's identity, she must provide photo identification before she can view her file.

A staff person will review the file before providing it to the woman to ensure any information about third parties is removed or blocked.

Files must be reviewed with a staff member, preferably the person who has the greatest responsibility for the file, present to answer any questions and/or provide support.

The woman will be provided with a quiet and private location to review her file with the designated staff. Only the woman and the designated staff person will be present. An exception to this will be made if the woman requires an interpreter.

The woman many not alter, duplicate, destroy or take any documentation from her file. Once she has read the file, she will return it to the staff person who will return it to its secure location.

The woman may request copies of the contents of her file, which will be provided to her within fifteen (15) business days.

8. File Retention and Storage

Policy Statement
X retains women's files and records for as long as required to fulfill the purpose for which the information was collected and to meet legal obligations. It stores such files and records safely and securely to protect client privacy.

Procedure:
[Pick and choose which of these apply to you.]
Files will be either under direct staff control or contained in a locked file system.

Only authorized individuals will have access to the locked file system that contains women's files.

The Centre will maintain appropriate technical and organizational safeguards including secured filing areas, confidentiality commitment (made by all staff), limited access and alarmed security systems in all locations where personal information is stored.

Files and records containing personal information will remain on the Centre's premises unless a counselor is meeting with a woman offsite or they must be removed to comply with a court order.

Files that are removed from the office will be returned to their secure storage location as soon as possible upon their return to the office. If they are removed to comply with a court order, a copy will be made and stored on site.

All computers that contain personal information about women receiving services will be password protected and will return to auto lock if unused for 5 minutes.

Computers will have current anti-virus and firewall protection.

Computerized records will be backed up regularly. Backup disks and tapes will be stored in a secure manner.

Because telephone messages may contain personal information, voice mail boxes will be password protected.

Personal information will be faxed or emailed only when no other method of delivery is available or meets the time requirements of the situation.

Fax cover sheets containing a confidentiality clause will always be used when faxing personal information.

When emailing, staff will contact the recipient by telephone before sending the email to confirm that s/he is the correct person and to confirm the email address.

Personal information will not be emailed using email distribution lists.

Emails containing personal information will be printed upon receipt and then deleted from the computer.

When staff meet with women offsite, they will take only the portion of the file that is required for the meeting and will keep it in their possession at all times.
If possible, staff will take copies of files or records and leave the original in the office.

If the personal information is stored on a laptop or other electronic device, it will be password protected and staff will keep it with them at all times.

If the file or record is in paper format, it will be kept in a locked briefcase.

If staff cannot keep the file or record with them for any period of time, it will be placed in a secure location such as a locked filing cabinet.

If files or records must be left in a car, they will be locked in the trunk.

Offsite computers that contain personal information about clients will not be used by other people, including family members.

Client files and records will not be saved on the hard drive of a home computer.

Staff will log off or shut down their computer when they are not using it.

Paper files and records will be stored in a locked space (desk drawer, filing cabinet) when they are not being used.

Staff will report the loss/theft of any files to the Executive Director or her designate immediately.

The Executive Director or her designate will determine the appropriate course of action, which may include contacting the police, conducting a search and/or notifying the client(s) whose personal information is missing.

9. Informed Consent

Policy Statement
X will take all possible steps to obtain informed consent from clients with respect to any matters related to their records and, in particular, to the disclosure of their records to any other agency or individual.

Clients receiving services using electronic communication such as text messaging or counselling via an online platform will sign a specific informed consent form after a discussion with her counsellor.

The Centre will ensure that information provided to clients is available in multiple languages, at various reading levels and in different formats as needed to increase accessibility.

Procedure
Informed consent is when a woman voluntarily agrees to do something or to allow something to happen after she has been advised about the possible risks and benefits and has had an opportunity to have reasonable questions answered.

Express consent is when a woman specifically agrees to do something or to allow something to be done.

Implied consent is when a staff person can conclude from the circumstances that a woman would agree to do something or to allow something to be done.

Both express and implied consent can be provided either orally or in writing.

In order to ensure accountability and transparency, X endeavours to secure consent relating to the release of women's files or personal information in written form whenever possible.

Signed written consent forms are placed in women's files for ongoing reference, review and, when appropriate, revision or cancellation.

X makes every effort to obtain express informed consent for the release of women's files or personal information unless there is an extremely urgent situation involving a woman's safety when staff are confident they have her implied consent.

10. Client communication

Policy:
When a woman contacts the Centre for services, the intake process will include a discussion about how the woman wants to communicate with the Centre.

The woman will sign an informed consent form for whatever methods of communication are agreed upon.

Procedure:
When a counsellor does intake with a new client, she will review the communication options that the Centre can provide for communication initiated by the Centre and communication initiated by the woman. This includes, but is not necessarily limited to:

- Telephone
- Email
- Text message
- Other (please list)

The counsellor and client will also discuss:

- The Centre's hours of operation
- The timeframe in which the Centre commits to responding to telephone messages, email or text messages
- Where the client can turn for support outside the Centre's hours of operation
- Communication safety planning (eg. Is it safe to leave a message on a telephone answering system?)

The client will then sign an informed consent form that details what forms of communication she and the Centre will be using.

11. Safety planning with clients about use of social media/technological communication

Policy:
The Centre supports all women who use its services in developing safety plans as appropriate and necessary. This safety planning addresses safe use of technology, including safety when accessing services through technology.

Procedure:
All safety planning with women is unique to each woman's situation, including technology safety planning. Some common elements of technology safety planning include:

- Separating phone, email and other accounts from the abuser, if they were shared in the past
- Checking for spyware installed on electronic devices
- Removing "cookies"
- Increasing privacy settings
- Removing GPS from smart phone (unless the woman needs it for her own safety, for example, when calling the police in an emergency)
- Changing passwords for all devices on a regular basis and keeping passwords private
- Keeping devices such as tablets and smart phones locked and in a private place
- Clearing browser history regularly
- Minimizing the amount of personal information shared on social media
- Considering how any social media posts, email/text message communication could be used in a harmful way (eg as evidence in a criminal trial)
- Using www.techsafety.org as a resource for safe use of technology

12. Screening clients for delivery of services using technological communication

Policy: Before technology-based services are offered to a woman, she will be screened to ensure she is appropriate for such services, with her safety and privacy being of the highest concern.

Procedure:
When screening a woman, the counsellor shall consider the following factors, as well as any others that are appropriate in the circumstances:

- The woman's private access to her own electronic devices
- Her skill and comfort level using technology
- Her willingness to engage in safety planning for her use of technology
- Her willingness to follow the terms contained in the informed consent form
- Her understanding of the importance of setting and following boundaries in her use of technology to obtain services from the Centre

13. Effective communication using technology

Policy:
The Centre acknowledges that communication using technology is different from face to face or telephone communication and works to ensure that all staff have the skills they need to communicate effectively using a variety of technologies.

Procedure:
Humour, sarcasm and anger can be easily misinterpreted in technology-based communication, so should be used minimally or not at all.

Complex and nuanced discussion is generally not suited to text or even email communication, so this should be limited as much as possible.

Staff should not use short forms or acronyms unless they already know the client is familiar with them.

Staff should establish with the client whether a communication is intended to be one- or two- way. (For example, staff should tell the client whether a response is expected to a text message telling the client when her next appointment is.)

The purpose of the communication should be briefly but clearly set out in the subject line or at the top of the communication. (For example: Confirming next appointment OR Checking in.)

Staff should confirm response times with clients.

A safe word should be established between the counsellor and the woman, which the counsellor can ask the woman to share if there are any concerns the person on the

other end of the technology is not the woman or is the woman but she is not in a safe or private situation.

INFORMED CONSENT TO USE ELECTRONIC COMMUNICATION

Centre Information

Name:
Address:
Email:
Phone (as required for service delivery):
Website:

(Name of Centre) has offered to communicate using the following forms of electronic communication (check all that apply):

Email
Text messaging
Social media (specify)
Videoconferencing (specify platform)
Website/portal
Other (specify)

Client acknowledgement and consent:

I acknowledge that I have read and fully understand the risks, limitations, conditions of use and instructions for use of the selected electronic communication services as described in the Appendix to this consent form.

I understand and accept the risks associated with the use of the selected electronic communication services as outlined in the Appendix to this consent form.

I consent to the conditions and will follow the instructions as outlined in the Appendix as well as any other instructions that (Name of Centre) may impose at any time.

I acknowledge that either the Centre or I can end this consent or the delivery of electronic communication services at any time.

I have had the opportunity to ask questions, all of which have been answered to my satisfaction.

Client name:
Client phone number (as required for service delivery)
Client email (as required for service delivery)

Client signature: Date:

Witness signature: Date:

CONSENT TO USE ELECTRONIC COMMUNICATION
Appendix

Risks of using electronic communication

The Centre will use all reasonable means to protect the security and confidentiality of information sent and received using electronic communication. However, the Centre cannot guarantee the security and confidentiality of electronic communication because:

- Use of electronic communication can increase the risk of information being disclosed to third parties
- It is not possible to completely secure information when using electronic communication
- Online service systems may have a legal right to inspect and keep electronic communications that pass through their system
- Electronic communication can introduce malware into a computer system
- Electronic communication can be forwarded, intercepted, circulated, stored or changed without the knowledge or permission of the Centre or the client
- Even if both the sender and recipient delete copies of electronic communication, back-up copies may exist on a computer system
- Electronic communications may be disclosed in accordance with a duty to report or court order

If the email or text is used as an e-communication tool, the following are additional risks:

- Email, text messages and instant messages can more easily be misdirected, resulting in increased risk that they could be received by unintended and unknown recipients
- Email, text messages and instant messages can be easier to falsify than handwritten or signed hard copies. It may not be feasible to verify the true identity of the sender or to ensure that only the recipient can read the message once it has been sent.

Conditions of using electronic communication services:

- The Centre cannot and does not guarantee that electronic communications will be reviewed and responded to immediately. The Centre commits to responding to electronic communication within (fill in what your response commitment is)
- Electronic communication services should not be used to emergency matters
- It is the client's responsibility to follow up with the Centre if she has not received a response to her electronic communication within the guaranteed period of time
- The Centre may forward electronic communication and any information contained in that communication to staff involved in the delivery of services to the client

- The Centre will not forward electronic communication and any information contained in that communication to third parties without the client's express, informed, written consent, except as required by law
- The client is responsible for informing the Centre about any types of information she does not want sent via electronic communication. The client can modify this list at any time
- The Centre is not responsible for information loss or breaches in confidentiality caused by technical failures with the client's software or internet service provider

<u>If electronic communication services include email, instant messaging and/or text messaging:</u>

- The Centre and the client shall include a brief description of the communication in the subject line and the client's full name in the body of the message
- The Centre and the client shall take precautions to preserve the confidentiality of electronic communications by using screen savers and safeguarding passwords

I have reviewed and understand all the risks, conditions and instructions described in this Appendix:

Client signature:
Date:

Witness:
Date: