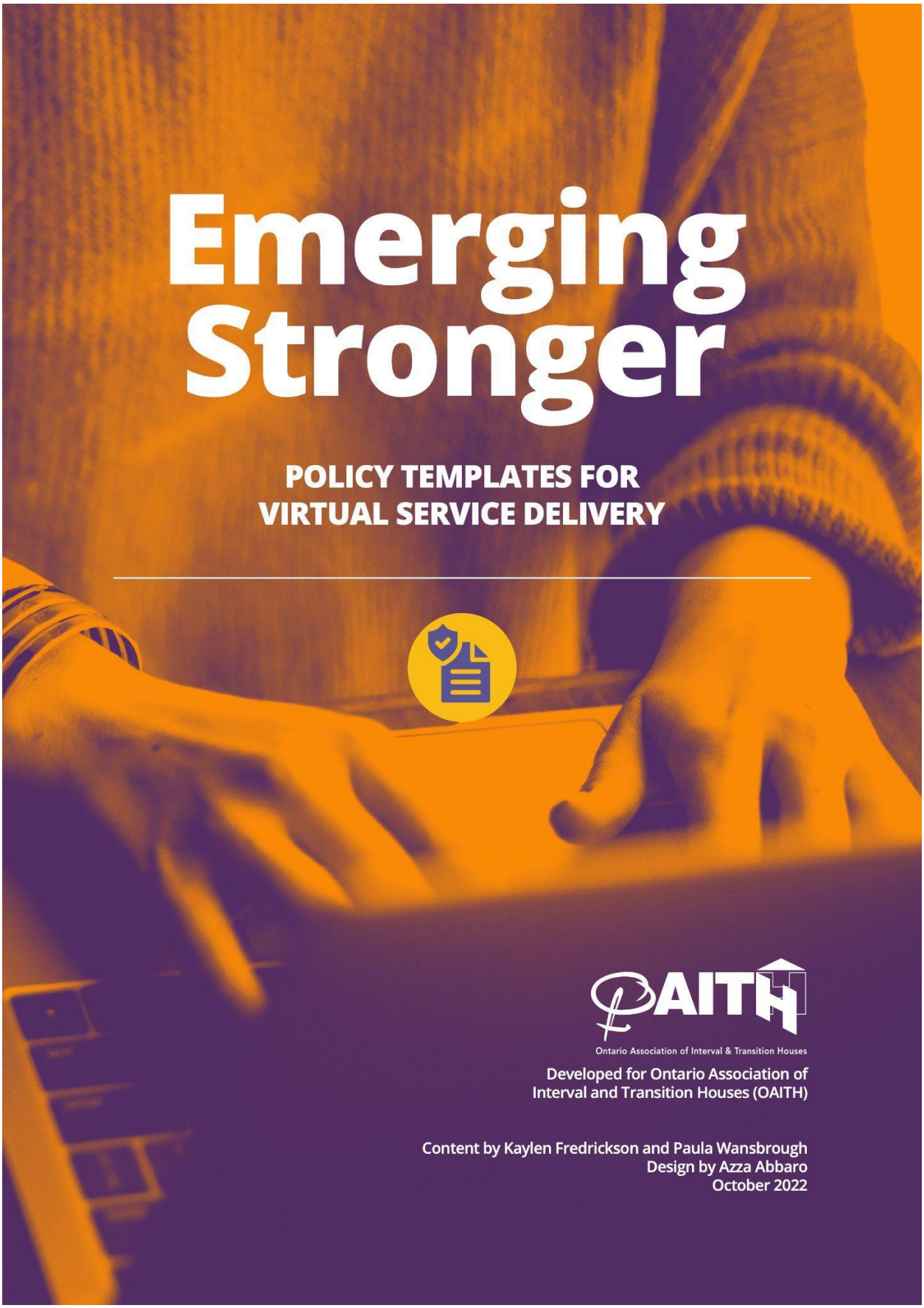

Emerging Stronger

POLICY TEMPLATES FOR VIRTUAL SERVICE DELIVERY

Ontario Association of Interval & Transition Houses

Developed for Ontario Association of Interval and Transition Houses (OAITH)

Content by Kaylen Fredrickson and Paula Wansbrough
Design by Azza Abbaro
October 2022

Acknowledgements

The Emerging Stronger: Virtual Service Delivery project consists of promising practices, policy templates and a resource list, which are available at https://www.oaith.ca/oaith-work/digital-safety.html

Emerging Stronger was prepared on behalf of the Ontario Association of Interval and Transition Houses (OAITH), a coalition of first stage emergency women's shelters, second stage housing organizations and community-based gender-based violence (GBV) organizations who work towards ending all forms of violence and oppression against all women, girls and gender-diverse individuals. OAITH achieves this through training, education, advocacy, public awareness and government relations.

OAITH members led the development of the promising practices and policy templates by participating in a survey, focus groups and interviews. Their time and candor is greatly appreciated. Thank you to all agencies that participated:

Aboriginal Shelters of Ontario
Alternatives for Women
Barbra Schlifer Commemorative Clinic
Bethesda House
Cornerstone Family Violence Prevention Centre
Domestic Abuse Services Oxford
Family Transition Place
Faye Peterson House
Green Haven Shelter for Women
Haldimand & Norfolk Women's Services
Herizon House
Hiatus House
Inasmuch House - Mission Services of Hamilton
Ingamo Homes
Interval House of Ottawa
Interval House
Maplegate House
Mattawa Women's Resource Centre
My Friend's House
Naomi's Family Resource Centre
New Starts for Women
Nova Vita Domestic Violence Prevention Services
Red Door Family Shelter
Sandgate Women's Shelter of York Region Inc.
South Asian Women's Centre
The Redwood
Three Oaks Foundation
Women's House Serving Bruce and Grey
Women's Place of South Niagara
Yellow Brick House
YWCA Sudbury Genevra House

This project has been funded by Women's Shelters Canada.

For specific information on online abuse and online safety planning, see the OAITH training, "Gender-Based Violence, Technology & Safety", also available through https://www.oaith.ca/train/training.html.

Table of contents

When Developing Policies for Virtual Services

- Get everyone on the same page
    - Create a glossary of terms and make sure everyone in your agency understands what is meant by these terms. In this document, we have included our own glossary, but your team might use different terms.
- Adapt current policies
    - Your current policies cover safety and client privacy for client services. They can be expanded or adapted to incorporate the specific considerations for virtual services.
- Test run the technology before you write the policy
    - As you integrate new tools, before creating policies, test the technology with service providers and survivors to determine what steps are necessary to protect survivors, service providers and the agency.
- Train service providers
    - Make it clear to service providers how policies tie to the agency's mandate and commitment to survivors.
    - Recognize that your service providers may use a technology in their personal lives and, because of this, may feel they don't need training. However, the appropriate settings and strategies for using an application in a GBV setting will likely be different from personal use.
    - Service providers will need ongoing training to build confidence and stay on top of upgrades to the technology, changes in abuse tactics and new strategies for service delivery.
- Recognize service provider expertise
    - External trainers may not fully understand the risks a technology can present for survivors and GBV service providers nor the realities of survivors' lives.
    - Trainings that make space for participants to share their knowledge and strategize with the technology expert on how to use the technology most effectively with survivors improves adherence to policies and procedures.
    - Consider performing your test run of the technology with one service provider team who can become internal experts and contribute to training service providers on other teams.
- Prepare for ongoing changes
    - Make a schedule and identify who is responsible for revisiting policies that are tied to virtual services. Because every secure application is updated

frequently, the associated policy may require updating. Reputable vendors will provide an overview of updates.
    - When a vendor changes an application's privacy policy, review their new policy as it applies to your agency's use of the technology.
    - When you change from one vendor or application to another (e.g. move from GoToMeeting to Zoom for video calls), you may need to update the procedures associated with the relevant policy.

The following policy templates are designed to be easily adapted to your agency's policy manual as many of these policies build on primary concerns for every GBV agency. Each template begins with a commitment or value that is common in GBV agency mandates, followed by context as to why the specific policy is required as well as general procedures.

Glossary

Application or app: A software package created by a vendor that enables a specific type of online activity (e.g. Outlook is an email application; Zoom is a video calling application)

Communication technology: Platforms that allow people to engage with one another online (e.g. social media, video calling, chat, text, email); while all communication technology can be categorized into different platforms, not all platforms are concerned with communication (e.g. database platforms are not); communication technology almost always directly and passively accumulates data about the people that use it

Device: Any personal equipment that is connected to the internet (and thus, other devices) or has the potential to do so, including desktop computer, laptop, mobile phone, tablet, assistive devices, smartwatches, fitness devices, children's toys; may extend to vehicles, virtual assistants, smarthome utilities and appliances

Passive data: Also known as incidental data, this is information about users that is automatically collected by an application, usually without the user knowing and can include data that could be used to identify the user, such as IP address, geographical location, time of action; an application's privacy policy should explain what passive data is collected; sometimes an application's settings can minimize passive data collection; passive data collection often pays for "free" applications because this data may be sold to companies or used to market other services

Platform: A specific type of online activity (e.g. video calls, chats, text)

Vendor: A company selling or offering an online tool or app for "free" (see: "passive data") (e.g. Google, Microsoft)

Virtual service: A category of online service (e.g. online counselling)

Virtual service delivery: Providing services online, usually using communication technology

Virtual service delivery format: Services delivered online by an agency on a platform (e.g. video calling in groups and individually); an agency may begin the service using one application but over time might change to another (e.g. begins with Zoom and then changes to Google Meet)

Privacy Considerations When Selecting Technology

Policy statement

Agency name is committed and legally obligated to securely manage the personal information of survivors, service providers and other stakeholders. This commitment extends to communication technology (e.g. video calling, chat/text messaging, email, social media) used for virtual service delivery.

Because communication technology often passively collects user data (e.g. record of interaction, IP address, user location), Agency name recognizes that failing to conduct a thorough investigation of an application before it is used with survivors will violate client confidentiality and may put survivors and service providers at risk of injury or death.

Agency name will thoroughly investigate the data collection aspects of any application prior to using it for the virtual delivery of services.

Procedure

When selecting technology Agency name service providers will determine if it:

- Allows Agency name to control the information that is collected about users
- Allows Agency name to control how and where the data is backed up
- Allows for anonymous user accounts
- Does not collect information on survivor's device or accounts
- Cannot access passive data (information about users) or content of conversations

When considering a new technology, an appropriately skilled person engaged with Agency name will research any security or other risks associated with the technology, including but not limited to a review of the associated privacy policies.

When an application that is new to Agency name is selected, the leadership team will develop a policy to guide service providers, which will include how to manage client crises that occur while using it.

Agency name service providers will be trained on the technology's security and privacy measures. This may include:

- User accounts and password management
- Adjusting privacy settings
- Data deletion

Agency name will identify a team member who will be responsible for re-assessing the technology's privacy policy and other features under these circumstances:

- On an annual basis
- If the privacy policies change
- If security issues are suspected

Safe Access to Virtual Services

Policy statement

In keeping with our commitment to fair and equitable access to our services, Agency name uses different communication technologies to reach, communicate with and support survivors.

However, because communication technology often passively collects user data (e.g. record of interaction, IP address, user location), Agency name recognizes these applications involve risk for end-users. Some applications have very limited use with most survivors because of associated risks. Some may pose greater risk for a survivor given the survivor's specific circumstances. As a survivor's circumstances change, the risk of using technology may also change.

When offering virtual services to clients, Agency name service providers will support survivors to select communication technology that minimizes risk to the survivor, other survivors using Agency name services who may be impacted (e.g. video call groups) and Agency name service providers.

Procedure

Service provider training

In order that service providers may properly assess whether a communication technology may be appropriate for a survivor, Agency name will ensure service providers are trained on:

- Online safety risks generally
- The specific risks associated with our virtual services and the technology we use
- How Agency name minimizes risks associated with our virtual services (e.g. the selection and set up of an application; policies, procedures and practices, including the careful management of survivor data), and
- How service providers can support survivors to minimize risk

Because technology changes rapidly, training will be ongoing. In particular, service providers will be trained when there are changes to technology we use, changes in abuse tactics and changes to service delivery practices.

High risk circumstances

If a survivor is deemed at high risk for abuser interference with their device(s) and/or account(s) (e.g. indications of spyware) or impersonation (e.g. previous history of such acts), Agency name service providers will:

- Guide the survivor to lower risk communication methods (e.g. phone) and service delivery (e.g. in-person), at least temporarily, and
- Seek ways to improve the survivor's access to safe technology (e.g. new phone, new email account, survivor visits satellite site or partner agency for video calls)

Any decision to use a virtual service with a survivor who is at high risk must be discussed with a supervisor before proceeding.

Once a survivor's risk has decreased, Agency name service providers may revisit virtual service options.

When risk is lower

When Agency name service providers have determined a virtual service and an application has lower risk for a survivor and the survivor has provided informed consent to use the service (see policy: Informed consent for virtual service delivery options), service providers will develop an individualized safety plan for the survivor for using the application.

This plan will include:

- A process to identify the survivor in text-based communications
- A process for the survivor to indicate during a live session that their circumstance is not safe, and
- What Agency name service provider will do if the survivor ceases to communicate during a live session

Agency name service providers will continuously check in with survivors about their safety as they use our virtual services.

This will include:

- Checking in with a survivor throughout each live session (e.g. during a video call or chat conversation)
- Revisiting the survivor's technology safety plan to confirm that the virtual service and safety processes are still suitable

Informed Consent for Virtual Service Delivery Options

Policy statement

Agency name is committed to empowering survivors to select virtual services that are appropriate to their individual circumstances and that minimize their risk of further violence.

However, because communication technology often passively collects user data (e.g. record of interaction, IP address, user location), Agency name recognizes these applications involve risk for end-users. Some applications have very limited use with most survivors because of associated risks. Some may pose greater risk for a survivor given the survivor's specific circumstances. As a survivor's circumstances change, the risk of using an application may also change.

All individuals accessing Agency name virtual services will be informed about the associated risks with the applications we use and, when Agency name conducts virtual services with a survivor, the survivor will first confirm their understanding about the service and then consent to using it.

Procedure

Service provider training

In order that service providers may give survivors the information they need to consent to a virtual service, Agency name will ensure service providers are trained on:

- Online safety risks generally
- The specific risks associated with our virtual services and the applications we use, and
- How Agency name has minimized risks associated with our virtual services (e.g. the selection and set up of an application; policies, procedures and practices, including the careful management of survivor data)
- How service providers can support survivors to minimize risk

Because technology changes rapidly, training will be ongoing. In particular, service providers will be trained when there are changes to technology we use.

When a survivor initiates contact

When a survivor initiates contact using Agency name virtual services (e.g. email, social media, chat, text), Agency name will provide a standardized message for service providers to share with the survivor that briefly describes the risks associated with the service or platform (e.g. “Email is not a secure way to share personal information.”). This may also include information about mandatory reporting obligations.

- **When a format is not used with survivors:** When Agency name has determined that a platform is too high risk for use with survivors (e.g. email, social media), the standardized message will refer the survivor to safer methods of contact (e.g. telephone, encrypted chat) for support.
    - If the survivor continues to contact Agency name through this platform, service providers will continue to urge the survivor to use alternative methods of contact using a standardized process.

- **When a format is used with survivors:** When Agency name has chosen a platform to use with survivors (e.g. encrypted chat) and a survivor initiates contact, Agency name will seek informed consent from the survivor.

Supporting survivors to provide informed consent

Agency name service providers will ensure the survivor (and, in the case of a minor, their guardian) understands the service requirements, service expectations and associated risks.

Agency name will aid service providers to ensure that the language they use to explain the virtual service, the application and associated risks is appropriate and understood by the survivor, recognizing that knowledge about and comfort with technology varies from person to person.

Video Calls

Policy statement

Agency name is committed to supporting survivors. Agency name is also committed to providing survivors with safe services and legally obligated to manage their personal information appropriately.

Video calls may create records of exchanges that an abuser may gain access to, potentially endangering the survivor. As well, an abuser may be present but not visible during a video call with a survivor, which may endanger the survivor, Agency name service providers and others participating in the meeting.

When conducting video calls with survivors, Agency name service providers must commit to specific technical requirements and user procedures.

Procedure

Agency responsibilities

Agency name will select a video call application that meets agency privacy requirements and will adjust settings appropriately. The agency will stay up-to-date on the security and other features of this application (see policy: Privacy considerations when selecting technology).

Agency name will train service providers on the safe and effective use of the video call application. This training must continue when there are upgrades to the application or new information related to the application or platform.

Agency name will ensure that

- Video calls with groups of survivors will be facilitated by two service providers
- Service providers have supervisory support and frequent opportunities to debrief, especially after high risk situations, detailed disclosures or crises.

Service provider responsibilities

Agency name service providers will only use the agency's video calling account when communicating with survivors.

Prior to selecting video calling as a service delivery method with a survivor, Agency name service providers will assess the survivor's risk (see policy: Informed consent for virtual service delivery options).

Specific to video calling when assessing risk, Agency name service providers will determine:

- If the abuser and the survivor live in the same place the video call will occur
- If the device and the account that is being used for the video call may be accessed by the abuser or is used by other people

When video calling with a survivor, Agency name service providers will establish an individualized safety plan (see policy: Safe access to virtual services).

To protect survivors' privacy, when using video calling with survivors, Agency name service providers will:

Setting up

- Use limited descriptors when setting up meetings in the video call application (i.e. no identifying information)
- Co-facilitate group video calls with survivors, designating one facilitator to manage and monitor access to the call as well as survivor emotional and physical safety
- Use privacy settings in the application to manage access to the call (e.g. passcode, waiting room)

Support survivors to

- Avoid data records (e.g. use web-based version of the application) and eliminate data records of the video call (e.g. delete video call link from email or text)
- Change identifying information (e.g. changing screen name to initials or first name only)
- Use headphones during the call

During the call

- Log into the meeting prior to survivors' arrival time
- Send the survivor the video call link
    - Manually, excluding the date and time, using the communication method decided upon with the survivor
    - Only when the service provider has started the meeting

- Screen all participants before they join the video call to confirm their identity
- Never record a meeting
- Never require a survivor to share their screen
- Avoid the use of chat features
- Use a language interpreter rather than closed captioning

At the end of the call

- Remain in the meeting until all others have exited
- Delete any records associated with the meeting afterwards (e.g. chat transcripts)

After any high risk situation, detailed disclosure or crisis during a video call, service providers will debrief with their team or supervisor.

Chat

Policy statement

Agency name is committed to supporting survivors. Agency name is also committed to providing survivors with safe services and legally obligated to manage their personal information appropriately.

If a chat application is not set up to meet certain requirements, it will create records of the exchange that an abuser may gain access to, potentially putting the survivor at risk. Even when using an encrypted chat application, a survivor may be at risk if the abuser sees the session (e.g. abuser has installed spyware on their device, gains access to the survivor's device during the session). As well, an abuser may use an agency's chat service to impersonate or inquire about a survivor.

When using chat to engage with survivors, Agency name service providers must commit to specific technical requirements and user procedures.

Procedure

Agency name will

- Select a chat application that meets agency safety and privacy requirements. The agency will stay up-to-date on the security and other features of this application
- Train service providers on the safe and effective use of the chat application. This training must continue when there are upgrades to the application
- Provide and maintain accurate safety information and terms of use about the chat service for survivors on the agency website

Agency name service providers will

- Use a designated account with the chat application when communicating with survivors
- Use a chat handle that does not identify the service provider (e.g. initials, alias)
- Never take a picture or screenshot of a chat session

Beginning a chat session

Consent: When a survivor initiates a chat session, the survivor will be directed (manually by service providers or automatically via the chat application) to the terms of use. The survivor

must consent to use the service before Agency name service providers may proceed with support.

Safety plan: Agency name service providers will confirm with the survivor that they are in a safe location and together they will determine how the survivor will indicate if they must quickly leave the session. During the session, service providers will check in with the survivor about their safety.

Limitations of service: Agency name service providers texting with survivors will limit their exchanges to topics defined by the agency (e.g. referrals, grounding techniques, check ins). Agency name service providers will explain the limitations to survivors.

Disclosures, crises and high risk situations

If Agency name service providers believe a chat user is in a high risk situation, they will provide the survivor with options (e.g. taxi pick up, police intervention).

If a survivor begins to provide a detailed disclosure, Agency name service providers will remind the survivor about the potential risks and limitations of the service, and provide alternative ways the survivor may seek support with Agency name.

If critical issues arise during a text session, Agency name service providers will follow the same procedure as set out for comparable crisis line exchanges.

After any high risk situation, detailed disclosure or crisis during a chat session, service providers will debrief with their team or supervisor. Agency name supervisors must ensure service providers have appropriate supports.

Current clients and when identity is known

Current clients who may need or desire ongoing support can use the chat if appropriate (see policy: Safe access to virtual services). Prior to suggesting chat as a service delivery method for such a survivor, Agency name service providers will assess the survivor's risk (see policy: Informed consent for virtual service delivery options).

If a survivor's identity becomes known (e.g. as a current client, or because the survivor shares their name and contact information) during a chat session, Agency name service providers will:

- Be aware that an abuser may be impersonating the survivor

- Seek to confirm the survivor's identity, if appropriate
- Not repeat information the survivor has shared in a previous in-person or virtual session in the current session
- Remind the survivor about Agency name service providers' duty to report children at risk

Abusive chat users

In situations in which a user is suspicious or abusive, Agency name service providers will take detailed notes and immediately notify a supervisor about this exchange.

- If Agency name service providers believe an abuser is impersonating a survivor or client, they will end the session using the standardized message: "The time for this session has come to an end." They may suggest that the user contact the crisis line for further support in case the user is indeed the survivor.
- If a chat user inquires if a survivor is using Agency name services, service providers will use the standardized message: "I don't have that information." Service providers will cease communication with the user.

Text

Policy statement

Agency name is committed to supporting survivors. Agency name is also committed to providing survivors with safe services and legally obligated to manage their personal information appropriately.

Text messaging can make a survivor vulnerable to surveillance by the abuser because it creates records of the exchange on the devices and with the mobile service providers for both parties. Even when using an encrypted text application, a survivor may be at risk if the abuser sees the session (e.g. abuser has installed spyware on their device, gains access to the survivor's device during the session). An abuser may also use text messaging to impersonate a survivor.

When text messaging with survivors, Agency name service providers must commit to specific technical requirements and user procedures.

Procedure

When texting with survivors, Agency name service providers will use only Agency name owned mobile phones. Agency name devices will not back up to the cloud and location tracking will be turned off.

Prior to selecting text as a communication method with a survivor, Agency name service providers will assess the survivor's risk (see policy: Informed consent for virtual service delivery options).

When texting is selected as a communication method with a survivor, Agency name service providers will establish an individualized safety plan (see policy: Safe access to virtual services).

Limitations of service

Agency name service providers texting with survivors will limit their exchanges to topics defined by the agency (e.g. referrals, grounding techniques, check ins).

When Agency name service providers text with clients:

- They will not create contacts for clients
- They will engage only in communication the survivor has consented to
- They will not share personal information about themselves
- They will not name the survivor in the exchange or repeat personal information the survivor has shared in a previous encounter
- They will discourage the client from providing any identifying information, including disclosures

If critical issues arise during a text session (e.g. survivor or other person's risk of injury or death, potential impersonation, duty to report a child at risk), Agency name service providers will follow the same procedure as set out for comparable crisis line exchanges.

Abusive text users

In situations in which a user is suspicious or abusive, Agency name service providers will take detailed notes and immediately notify a supervisor about this exchange.

- If Agency name service providers believe an abuser is impersonating a survivor or client, they will end the session using the standardized message: "The time for this session has come to an end." They may suggest that the user contact the crisis line for further support in case the user is indeed the survivor.
- If a chat user inquires if a survivor is using Agency name services, service providers will use the standardized message: "I don't have that information." Service providers will cease communication with the user.

After a text messaging session

Immediately upon the completion of a text exchange, in most cases Agency name service providers will delete the conversation from the Agency name device.

The exception to this is when there may be critical issues they must discuss with their supervisor and the record of the exchange will be necessary for this discussion. In this case, service providers will speak with a supervisor immediately following the session.

Email

Policy statement

Agency name is committed to supporting survivors. Agency name is also committed to providing survivors with safe services and legally obligated to manage their personal information appropriately.

Email can make a survivor vulnerable to surveillance by the abuser because it creates multiple records of the exchanges. Copies may exist on multiple devices, with the email providers, and possibly with networks or cloud-based back-ups for both the sender and receiver. These copies create opportunities for the messages to be intercepted. Email messages can also easily be sent to the wrong address or forwarded to other addresses. An abuser may also use email to impersonate a survivor.

When emailing with survivors, Agency name service providers must commit to specific technical requirements and user procedures.

Procedure

When emailing with survivors, Agency name service providers will use only Agency name owned devices. Agency name devices will not back up to the cloud and location tracking will be turned off.

Limitations of service

Agency name service providers emailing with survivors will limit their exchanges to topics defined by the agency (e.g. referrals, grounding techniques, check ins).

Agency name will develop a standardized message for service providers to share when a survivor seeks in-depth support through email. This message will include:

- A brief description of the risks associated with the service (e.g. “Given the challenges with email safety, our agency cannot provide personalized support this way.”).
- Safer ways Agency name provides support to survivors (e.g. telephone, encrypted chat).

Safety procedures

Prior to selecting email as a communication method with a survivor, Agency name service providers will assess the survivor's risk (see policy: Informed consent for virtual service delivery options).

When emailing is selected as a communication method with a survivor, Agency name service providers will establish an individualized safety plan (see policy: Safe access to virtual services) which may include:

- The survivor sets up an email account the abuser doesn't know about
- The survivor changes their password frequently
- The survivor logs out of email after every session

Both the survivor and service provider:

- Always start with a new message (no email threads)
- Use vague subject lines
- Delete emails, empty email trash

When Agency name service providers email with survivors, they will:

- Engage only in communication the survivor has consented to
- Discourage the survivor from providing any identifying information, including personal stories
- Direct survivors seeking more in-depth support to safer service options (e.g. telephone, in-person, encrypted chat)

When Agency name service providers email with clients, they will **not**:

- Share personal information about themselves
- Name the survivor in the exchange or repeat personal information the survivor has shared in a previous encounter
- Forward any email from a survivor

When Agency name service providers email with colleagues, they will **not**:

- Share personal information about clients

If critical issues appear in an email from an external source (e.g. potential impersonation; child, survivor or other person at risk), Agency name service providers will confer with their supervisor.

Deleting emails

Immediately upon the completion of an email exchange with a survivor, in most cases Agency name service providers will delete the email from their inbox and from their trash.

The exception to this is when there may be critical issues they must discuss with their supervisor and the record of the exchange will be necessary for this discussion. In this case, service providers will speak with a supervisor immediately. The email should not be forwarded for the purposes of supervision but instead reviewed in the service provider's account and deleted immediately.

Social Media Amendment

Policy statement

Agency name is committed to supporting survivors. Agency name is also committed to providing survivors with safe services and legally obligated to manage their personal information appropriately.

Messaging via social media can make a survivor vulnerable to surveillance by the abuser because it creates a record of the connection with our agency and a record of the exchange with both social media accounts. Even when the social media messaging is encrypted, an abuser may be using it to impersonate a survivor. In most cases, the social media vendor will have access to these messages as well.

Given the inability of Agency name to manage survivor's personal information in social media, Agency name service providers must commit to specific procedures when survivors seek support through this medium.

Procedure

Agency name will provide up-to-date information on our social media accounts on how survivors can access our services as well as the limitations of our service delivery via social media.

Agency name will develop a standardized message for service providers to share when a survivor seeks support through Agency name social media messaging accounts. This message will include:

- A brief description of the risks associated with the service (e.g. "Given the challenges with managing social media, our agency cannot provide personalized support this way.").
- Safer ways Agency name provides support to survivors (e.g. telephone, encrypted chat).

Agency name service providers will not provide any services directly to individual survivors via social media messaging. Survivors asking for support will be directed to safer service options (e.g. telephone, in-person, encrypted chat).