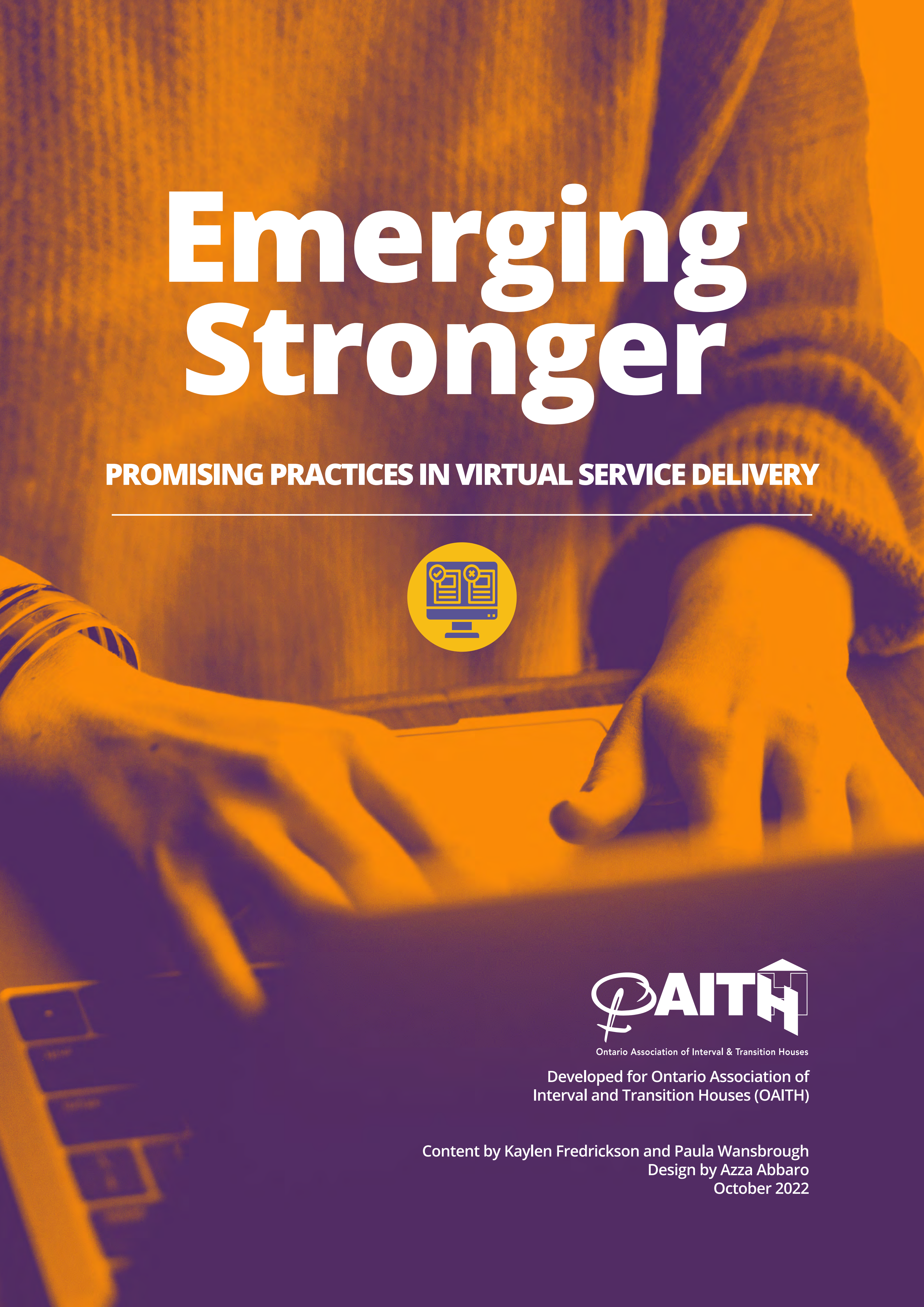


Emerging Stronger

PROMISING PRACTICES IN VIRTUAL SERVICE DELIVERY

OAITH
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

all of which are available at: 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

Please consider the environment before printing! If printing, here are some tips: https://gradient.postermywall.com/2021/07/06/how-to-print-edge-to-edge-on-your-printer/

Table of Contents

The Context

Virtual gender-based violence services can be a lifeline for survivors

- Expands access to service for current clients and reaches new audiences
- Increases accessibility for people who have disabilities, face barriers to travel or don't have childcare
- Some survivors feel safer and more comfortable using a virtual service than visiting an organization in person
- Text-based options are essential when an abuser may overhear a call to a crisis line
- Current clients can maintain contact and choose options that best fit their lives

But virtual services are not for everyone, all the time

- Some survivors don't have access to devices or internet and mobile services
- There are risks for survivors when using communication technology, in particular, abusers use this technology to monitor, harass and impersonate survivors
- The internet and mobile connections may be poor in rural and northern communities
- Many people find there are limits to the sense of connection that can be achieved virtually

It's a balancing act

With virtual services, GBV agencies have to weigh the value of offering support to survivors against

- **Possibly increasing the risk of violence:** the abuser may be using the technology to monitor the survivor
- **The proper management of personal data:** the communication technology will likely be actively and passively collecting user data
- **Their service providers' safety and well-being:** service providers can't know for sure who they are communicating with or who is just off-screen, there are limits to how much support they can provide, and an impersonating abuser may trick them
- **Sustainability:** how to offer virtual services safely and effectively for the longer term

Supporting Survivors to Select the Best Way to Connect

A new role for GBV agencies is to support survivors to select the virtual services that safely fit their unique circumstances.

Talk about the tech

- During intake and safety planning, talk with survivors about the abuser's access to their devices, their children's devices and the possibility of spyware
  - For online safety information, see the OAITH training, "Gender-Based Violence, Technology & Safety": https://www.oaith.ca/train/training.html

Get informed consent

- Describe to the survivor the ways you can stay in contact as well as the risks involved (see "Comparing the Risk of Virutal Services" chart on the next page)
  - Include low and no tech options, e.g. phone, in-person
  - Explain how a survivor can minimize and delete the data that is saved on their device or account
  - Set clear expectations with survivors about what kind of information you will discuss when using a specific virtual service

When using any virtual service with survivors

- Only use your organization's accounts and devices
- Plan with the survivor how they will
  - Identify themselves when using text-based formats
  - Let you know if they are no longer safe during an exchange, e.g. code word
- Prioritize survivor safety
  - Check in frequently to make sure it's still a safe option
  - The survivor knows the abuser best

Comparing the Risk of Virtual Services

FORMAT	SURVIVOR'S CIRCUMSTANCES	SERVICE ACTIVITY	RISKS	TO IMPROVE SAFETY
VIDEOCALL **medium risk**	***Low risk if*** • The survivor does not live with the abuser ***Requirement*** • The survivor has access to high speed internet connection, sound, mic and webcam ***Other recommendations*** • Children will not be present for the video call • Participants are in quiet, private spaces and use headphones	For one-on-one meetings and when needing to include a language interpreter Group sessions if no participants live with an abuser	• The abuser may be off-screen • The video call application may create a passive data record	• Choose a video call application that does not require the survivor to create an account or download an app • Use privacy settings when setting up meetings, send the link to participants once you have started the meeting excluding the time of the meeting, monitor who joins • Do not record, use the chat or have the survivor screen share • A survivor may choose to keep the camera off • For more privacy when children are in the home, the survivor can use headphones, join the meeting from their phone outside or in their car ***If the survivor lives with the abuser*** • The survivor may be able to video call from a trusted community service
ENCRYPTED CHAT APPLICATION **medium risk**	***Low risk if*** • The abuser does not have access to the survivor's devices ***Considerations*** • The survivor is comfortable with text-based communication • Less demand on internet bandwidth than video call	For grounding techniques, check-ins, referrals	• May create a record of the exchange on both devices • The abuser could impersonate the survivor	• Ensure that there is no record of the exchange when it ends (encrypted chat applications may auto-delete, otherwise both people must do this manually; show the survivor how to do this)

FORMAT	SURVIVOR’S CIRCUMSTANCES	SERVICE ACTIVITY	RISKS	TO IMPROVE SAFETY
EMAIL **high risk**	***High risk*** • Use only where there are no other alternatives for communication ***Risk decreases if*** • The abuser does not know about the email account and cannot guess the password • The abuser doesn’t have access to the survivor’s devices	***When no other option:*** For referrals, immediate action information, e.g. video call link	• Creates a record of the exchange on both devices • Creates passive data records on each person’s internet service provider, email application and email server • The abuser could impersonate the survivor • Email messages can easily be sent to the wrong person, forwarded	• 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 people always start with a new message (no email threads) • Both people delete emails, empty email trash
TEXT **high risk**	***High risk*** • Use only where there are no other alternatives for communication ***Risk decreases if*** • The abuser doesn’t have access to the survivor’s devices nor the mobile service account • Service provider offers an encrypted text application ***Consideration*** • An option when a survivor really needs support but doesn’t want to be heard or doesn’t have internet access	***When no other option:*** For grounding techniques, check-ins, referrals, immediate action information, e.g. video call link	• Creates a record of the exchange on both devices • Creates passive data records with the mobile provider • The abuser could impersonate the survivor	• Both people delete the conversation when it is finished • Neither person creates a contact for the other

FORMAT	SURVIVOR'S CIRCUMSTANCES	SERVICE ACTIVITY	RISKS	TO IMPROVE SAFETY
SOCIAL MEDIA high risk	***High risk*** • Use only where there are no other alternatives for communication ***Risk decreases if*** • The abuser doesn't have access to the survivor's devices or account • The application offers an encrypted messaging option ***Consideration*** • An option when a survivor really needs support but doesn't want to be heard	***When no other option or when encryption is used:*** Grounding techniques, check-ins, referrals, immediate action information, e.g. video call link	• Creates a record of the connection and the exchange on both accounts • Creates passive data records the social media vendor can access • The abuser could impersonate the survivor	• Both people delete the exchange and connection after each session • The survivor logs out of the application after every session • The survivor changes their password frequently • Both people implement the encryption option if available

Are You Considering Starting a New Virtual Service?

EXPLORING

When exploring new virtual services, consider conducting a needs assessment. Keep in mind that virtual services often reach different people than in-person services; meaning, existing clients' interest in virtual services may not capture the need present in your community.

What is the purpose?

- What need are you trying to meet?
- Who is the audience you are trying to reach? Consider:
  - Meeting people where they're at
  - Accessibility needs
  - Low tech options
  - Survivor choice

Can technology meet this need?

- What type of technology might work?
- Are there other ways to meet the need?

What may be challenging?

- What are the risks?
  - Can you mitigate safety risks for survivors?
  - Can you protect service providers?
  - Does the organization have the capacity to manage user data appropriately?
- How accessible will it be? (e.g. for people with disabilities, bandwidth and equipment requirements)
- Do you have the resources to ensure the new service is sustainable?
  - Does the organization have capacity for increased demand?
  - Is there a risk you'll promote a new service and then not be able to meet expectations?

Who can help?

- Who can help you assess the technologies available?
- What funding, donations and in-kind support could assist?
- Have other organizations tried this?
  - Can you talk with them about their experiences?
  - Can you collaborate?

PLANNING

Planning for a new virtual service means thinking about how the service will impact your organization and your clients. You want the right people to get involved in the planning to increase your likelihood of success.

How will the new service work with your other services?

Consult service providers about how they see the virtual service fitting in with existing services.

- Where do they see the need?
- How will the survivor's context impact their ability to participate in the virtual service?
- What are service providers' safety concerns for survivors and themselves?

Delivery model

Virtual and in-person services have different strengths and can appeal to different audiences for different kinds of communications.

In-person

- Build meaningful connections
- Provide a break from home life
- Reduces tech or internet barriers

Virtual

- Fast
- Reduces travel and childcare barriers
- Higher attendance for groups

In some cases, you might offer virtual and in-person services separately (e.g. participants can either sign up for virtual or in-person group counselling).

In other cases, think about a hybrid approach to a service where virtual and in-person formats are blended to use the strengths of both (e.g. meeting in-person for individual check-ins and virtually as a group, or having intake appointments in-person and follow-up appointments virtually).

Leadership and expertise

Who do you have inside and outside your organization that can champion the service?

- Consult with IT support
- Select vendors
- Coordinate training
- Capture learnings
- Create policies

Capacity

Adding a new service will mean an increase in workload as well as a new kind of work. Think about your capacity as an organization and if you're well-positioned to offer a high quality service that is sustainable.

- How will the organization handle increased demand on service providers' time and energy?
- What other resources need to be in place to support clients gained through new services?
- Do you plan to expand services over time?

Financial cost

Setting up a new service and maintaining it requires ongoing investments. Make sure your organization has the resources recognizing that with technology there will be continuous updates.

- Application, updates
- Fees and maintenance
- Equipment
- Training
- Service provider and supervisor time

Information management

Virtual services will involve recordkeeping, similar to in-person services. Applications may also passively collect data about service providers' and survivors' use of the technology.

- Research the application you will use and create an information management plan to keep information safe
- Understand which features of the technology allow you to limit the information collected and stored
- Train service providers on information management

Pilot testing and early evaluation

Before fully committing to technologies or processes, plan for a pilot test of the virtual service to see what works best. This is a crucial time to gather service provider and survivor feedback to ensure success.

IMPLEMENTATION

To start offering the service, take steps to clarify how it will work.

Prioritize client safety

- Help survivors make informed choices about virtual services
- Give strategies to minimize storage of sensitive information
- Be clear about what survivors can expect from a service

Set up support for service providers

- Who on your team will provide the service?
- How will supervisors help service providers adapt and debrief?

Offer service provider training

- Technology
- Delivery skills
- Information management
- Policies

Adapt policies

- Start with what you know: your existing policies are likely a great place to start
- Risks to plan for: interception, impersonation, privacy and confidentiality

Promote the service

- When will services be available?
- How will you describe it so that people understand what you are offering?
- How will people find out about the services?

Evaluate

- How will you collect data about the services?
- How will you measure success?

Considerations When Choosing Technology

Once a need for a particular virtual service is established and the right mode of delivery has been selected, choosing an application is the next step.

TIPS

- If there are free versions or free trials or low-cost entry fees, try them before you commit and see how the technology and tech support works. Avoid using free versions with clients as these likely access, store and sell user information.
- For guidance and buy-in, include service providers who will use the technology with clients in the selection process.
- Once a new technology is selected, practice before using it with clients.

Use these charts to compare the applications you are considering with regards to:

Cost

Privacy and Safety

Features

Equitable Access

Cost Comparison Chart

Application and vendor	Application purchase, fee package options	Set up fee, customization	Reduced fee for non-profit?	Ongoing user fees, upgrades, maintenance	Equipment required (may require upgrade)	Internet bandwidth requirement (may require upgrade)	Security measures (anti-virus, anti-malware software)	Training on how to use the application
Application option 1								
Application option 2								
Application option 3								
Application option 4								

Privacy and Safety Comparison Chart

Application and vendor	Option for anonymous users	Users are not required to log on through third parties (e.g. Google, Facebook)	If users are required to create their own accounts, what information is collected?	Can users easily change their settings and close their account?	Are there records of exchanges left on the users’ devices and accounts? If yes, how easily can records be removed?	What user data does the vendor have access to? Is the data encrypted?	Where does the vendor store user data? (Data will be governed by that country.)	If the data can be stored to the cloud, can this option be turned off?
Application option 1								
Application option 2								
Application option 3								
Application option 4								

Features Comparison Chart

Application and vendor	Multiple service provider accounts available	What tech support is available? What's the quality and is there a limit?	Access to training and resources	Other feature	Other feature	Other feature	Other feature	Other feature
Application option 1								
Application option 2								
Application option 3								
Application option 4								

Equitable Access Comparison Chart

Application and vendor	Easy to use	Accessibility options (e.g. large font, colour filters)	No account, download or app required	Respects lower bandwidths (e.g. calling in video by phone)	Integration of interpretation or translation services	Designed for non-profits	Privacy policy is under-standable	Does the vendor have any political alliances or history to consider?
Application option 1								
Application option 2								
Application option 3								
Application option 4								

Collecting Client Information

About client information

- Personally identifying information that is often collected by technology includes: name, address, ID numbers, date of birth, phone number, IP address, user name, email address, location
- Some information can be used to directly identify a person (like phone number), whereas others may be used together (like a combination of age, ethnicity and community where they live)
    - This information may come into unintended hands
        - **In your organization:** staff who do not need access, IT support
        - **Abuser:** may physically access the survivor's device or install spyware, impersonate the survivor to trick service providers, subpoena information from organization and tech service providers
        - **Application vendor:** may collect, store and sell information - read about user data in their privacy policy
        - **Hackers:** may attack database of organization or vendor

STEP 1: Only collect information you need.

The best way to ensure safety of information is to not collect it in the first place.

- Don't ask for personally identifying information if you don't need it
    - What information do we really need?
        - To connect the client to the right services
        - To make the right referrals
        - To satisfy funders
- Don't save content of conversations
- Don't collect or save any documentation of abuse (such as: photos, screenshots, recordings, etc.)
- Don't require users to create accounts or download apps
- Don't import information from an application into database
- Choose vendors that don't see or store passive data

TIPS

- Avoid creating forms from old ones which may ask too many questions.
- When deciding to collect information, imagine what the client's abuser might do with it (e.g. subpoena).
- Remember to always ask for informed consent before collecting any client data.

STEP 2: Collect as general information as possible.

Protect client privacy by using broader information categories.

- If you need some personal information, make it more general, e.g. clients select an age range instead of sharing their date of birth, select a region where they live instead of sharing addresses

STEP 3: Limit access.

Control where information is kept and who has access to it.

- Create unique usernames with strong passwords for any accounts
- Set up a clear structure for saving files containing client information to avoid files being saved in multiple places
- Ensure only those who need access to the most detailed information can access it. If less specific information is needed by someone, share aggregate data or de-identified data instead of access to the original files
- Store files in an encrypted database. Only share files through encrypted messaging or file sharing service

TIP

- Consider using passphrases, especially for shared security checks (e.g. to access a password-protected document or to join a video call). A long passphrase (often a few words together, like "yellowpencomputerfruit") is meant to be hard to guess but easy to remember. You can tell the passphrase to someone and avoid sharing it in writing, which decreases the risk of someone unintended seeing it.

STEP 4: Review and delete information regularly.

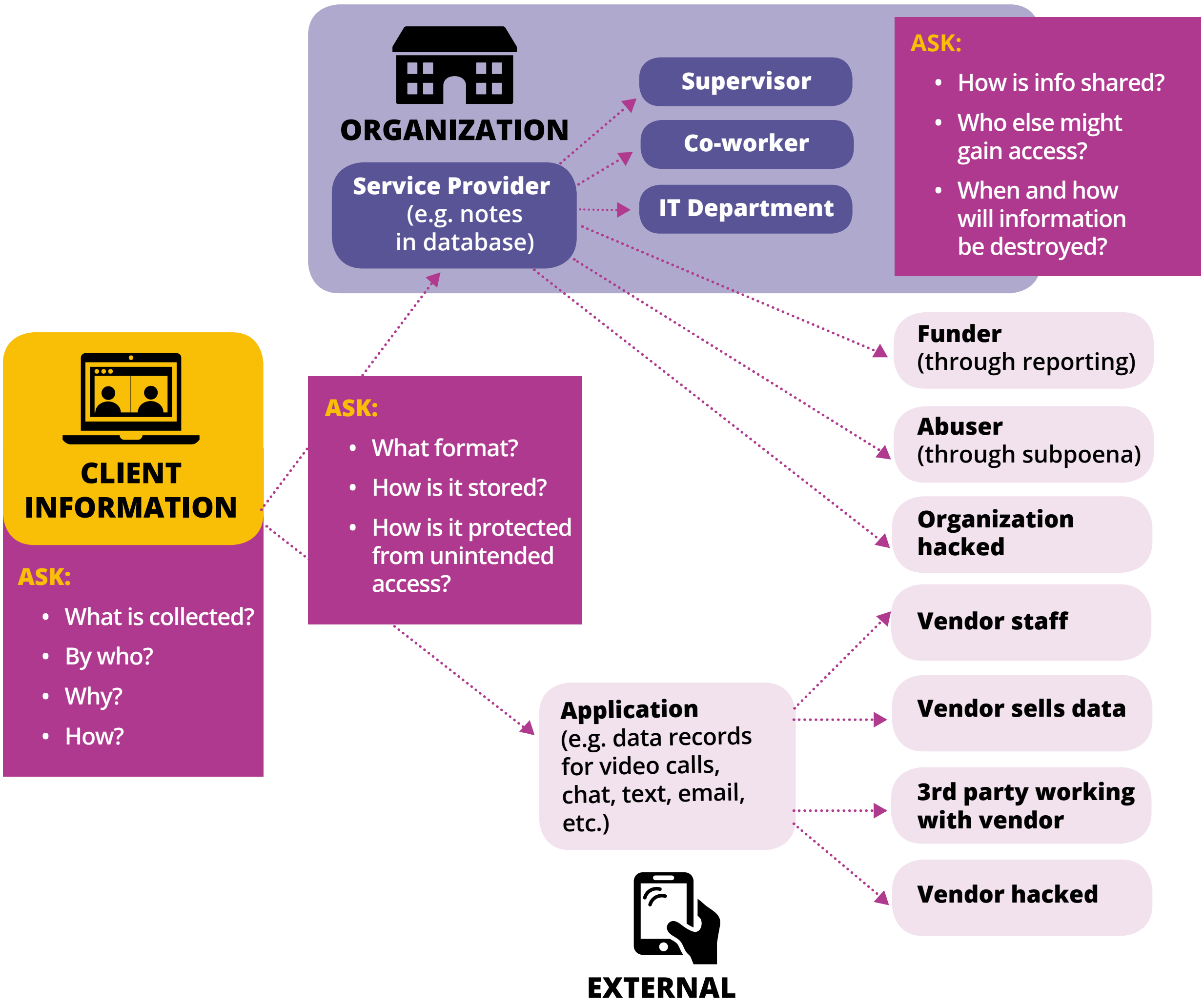
Create and follow clear policies and processes for when and how information will be deleted.

FUTURE STEPS: Talk to your IT support or connect with external IT supports.

When new situations or decisions arise, having someone with IT expertise to help you understand the security issues will make decisions clearer.

- Ask: Are there ways other people might see information shared in this way? How can we limit those weaknesses?

Are you facing a complex system of data collection and storage? Conduct a privacy impact assessment to understand the flow of information.



ORGANIZATION

Service Provider (e.g. notes in database)

Supervisor

Co-worker

IT Department

ASK:

- How is info shared?
- Who else might gain access?
- When and how will information be destroyed?

CLIENT INFORMATION

ASK:

- What is collected?
- By who?
- Why?
- How?

ASK:

- What format?
- How is it stored?
- How is it protected from unintended access?

Funder (through reporting)

Abuser (through subpoena)

Organization hacked

Application (e.g. data records for video calls, chat, text, email, etc.)

EXTERNAL

Vendor staff

Vendor sells data

3rd party working with vendor

Vendor hacked

Healthy Practices for Organizations

Recognize new demands on service providers

- Service providers need training to support their safe use of technology with survivors
- Assess comfort level with text-based communication (e.g. experience, fluency in written)
- Ensure time and support for text-based communication
    - May take longer and increase service demand
    - Service providers may read more explicit disclosures
- Provide debriefing opportunities for team members to manage stress and share strategies
- Create policies and processes and train your team on
    - Informed consent during virtual exchanges
    - Challenging situations, e.g. abrupt topic shifts, survivor stops responding
    - High risk situations, e.g. abuser interference or impersonation
    - Misuse of services

Who's there?

Service providers have less control in the virtual environment because they can't be sure who is on "the other end" (e.g. off screen, sending or receiving the message). Ways to manage concerns

In video calls

- The link to the call is sent to the survivor(s) after the meeting has started and does not include the time for the call
- Co-facilitation of groups, e.g. one person presents, the other person manages participants joining and leaving and responds to emotional and physical safety needs
- Participants share their surroundings and use headphones

In text-only formats

- Create a process for identifying the survivor
- Do not discuss information the survivor has shared in previous exchanges
- Delete any threads or message history

Service provider screen fatigue

- For meetings, use a mix of in-person, phone calls and video calls to break up screen time
- Support service providers to use breaks to get away from screens to reduce eyestrain and to move their bodies
- Provide ergonomically correct office equipment
- As a team
  - Discuss ways to limit the number of emails and virtual meetings
  - Establish and follow virtual communication etiquette (e.g. video cameras on in meetings, clear email subject lines including when you need a response)
  - For meetings with people joining both in-person and virtually, use a large screen in the meeting room so everyone can see each other
  - Ask each service provider about their preferences for virtual and in-person work
  - Pick up the phone for difficult communications, to ease confusion, or just to get away from the screen

Video Call Checklist

Is video calling the right option for this survivor?

□ They have access to the necessary technology

- High speed internet (Can they watch videos?)
- Device with webcam, sound and mic
- Nice to have: earbuds or headphones with mic

□ They have a safe and appropriate space

- The conversation will not be overheard by the abuser, children or others (e.g. survivor may join from their car or a non-profit close to their home)
- The location is quiet and private
- The survivor feels safe

Safety

□ Use a reputable video call application

□ Facilitate groups with a team member: one of you will focus on survivor safety, the other on the content and group dynamic

□ Before the video call, find a safe way to discuss online safety with the survivor (e.g. in person, phone)

□ Delete traces of the call, if the survivor has an account with the same service (e.g. Zoom) or vendor (e.g. Google)

□ Develop a signal that the survivor can use to indicate that the situation is not safe

□ You may wish to text the survivor just before the meeting to ensure it's still a safe time

Preparation

Prepare yourself (and your co-facilitator)

□ Accept that you have less control in the virtual environment. How can you make this easier for yourself? What will you do if there is a crisis?

□ Plan for things to take longer online: you may need to reduce or revise what you want to cover compared to in-person meetings

□ Book a quiet, private space for the meeting

□ Think about the background: What atmosphere does it create? Is any confidential information visible?

□ Adjust lighting so that you are clearly visible

□ Test the technology: the device, sound and internet connection

- Headphones or earbuds provide the best sound quality

- □ When booking the meeting within the video call application (e.g. Zoom), use a vague descriptor with initials only
- □ Have a backup plan if video calling doesn't work out

Prepare the survivor

- □ Learn how comfortable the survivor is with video calls
  - Offer and prepare to spend time during the first session helping the survivor get comfortable with the technology
  - If it's safe to do so, share a video calling tip sheet or link
- □ Explain security risks and the limits of privacy or confidentiality for video calls
  - How your organization mitigates risks (e.g. carefully selecting an application, using a waiting room or passcode)
  - How the survivor can mitigate risks (this will be specific to the individual)
- □ Explain the process
  - When you will send the link
  - If there will be a virtual waiting room and/or passcode

> ***TIP***
>
> **If email or text is safe for the survivor, send them the link after you have started the meeting**

- □ Suggest ways to make the meeting more pleasant
  - Appropriate lighting
  - Comfortable seating
  - Stress relieving supports, such as a pet, stress ball
- □ What will happen if the technology does not work
  - Troubleshooting tips (e.g. log out and back in)
  - Exchange phone numbers ahead of time and determine who will call who

For facilitators and survivors, right before the meeting

- □ Use the bathroom
- □ Try to eliminate distractions (e.g. turn off device notifications, put the kids in front of TV in another room)

To begin the meeting

- □ Check with survivors about the safety of their situation; reconfirm this throughout the meeting
- □ Support survivors to use only their first name or initials as their profile name
- □ Remind survivors of the process if the connection fails
- □ Describe the confidentiality of your setting; you may wish to show your location
- □ Review the confidentiality agreement
- □ To avoid creating records, do not record the meeting and avoid the chat

After the meeting

- □ You’re the host: chat with stragglers, be the last person to log out of the meeting
- □ If challenges arose in the meeting, debrief with your team or supervisor. What can your organization learn from this?

More Inclusive Video Calls

Connection issues

What to look for when selecting a video calling application

- Requires less bandwidth
  - Look at the recommended system requirements and test free options
- Offers a phone-in option for audio
  - Support survivors on how to use this feature ahead of time

If the connection is poor during a meeting

- Exit the meeting and join again
- Move to the phone-in option for audio
- Turn off video

When a survivor doesn't have a device or their home connection is poor, use a device in a private room at a safe service close to their home (e.g. other non-profit, public library)

Language interpretation in different settings

1 on 1 meeting

- The interpreter joins the video call with you and the survivor
- If it is spoken language interpretation, the survivor can choose if they would like the interpreter's camera on or off
  - If the interpreter will have their camera off, they can call into the meeting rather than join by the web link; their connection to the meeting will appear as a phone number (not a name)

Presentation or group session
For events with an instructor (e.g. yoga, art), with one or more spoken language interpreters

- **Option for any video calling application:** Requires that the survivor has access to a phone as well as a computer
  - The interpreter joins the meeting with everyone else
  - The interpreter phones the survivor they are interpreting for and provides interpretation over the phone while the survivor views the session

- **Option for paid Zoom accounts:** Requires that the host has a paid Zoom account and the survivor has access to a Zoom account (rather than web-based access)
  - Detailed instructions are provided on the Zoom website

For a survivor who needs interpretation to participate in a group discussion, make time for the survivor to hear the interpretation and share their question or comment with the interpreter who will relay it to the group.

Sign language interpretation in a group setting

- If there will be more than one interpreter, tell them if you will be spotlighting them so that the new interpreter can let you know when it's their turn to be spotlighted

Captioning

Ask survivors if captioning is helpful before assuming it is; an interpreter is likely the best choice

- Automated captioning feature option (only available in some applications)
    - Can make mistakes, especially if speakers have an accent or use less common terms (e.g. legal, culturally specific)
    - If possible, a team member provides corrections in the chat
- Human captioning option
    - Humans can also make mistakes!
    - Select a team member or third party to caption who is familiar with the terms used
- Prepare captioners with meeting documentation ahead of time
    - For confidentiality: Never share personal information, including names in the chat, as the chat creates a data record

Video calls with language interpretation checklist

Before the meeting

□ Book the interpreter well in advance, especially sign language interpreters (immediate service for some languages may be available for emergencies)

□ Interpretation takes time: plan for a longer meeting or less content

□ Provide the interpreter with documentation related to the meeting a few days in advance (e.g. agenda, facilitator names and roles, slides, forms, etc.)

□ Explain any acronyms and other unique terms

□ Ensure there will be really good sound and visual quality

□ Allow the interpreter to join the meeting ahead of time to check their connection

□ Ensure the interpreter can communicate with your team if there is a technical issue

During the meeting

□ Ask everyone to speak at a moderate pace

□ If there are slides, pause before changing slides to provide time for interpretation

□ If there is a form the survivor must read, send it to the interpreter (in advance, when possible) and screen share it so the interpreter can read it to the survivor

Implementing a Chat Service

Why offer a chat service

- Support survivors for whom phone or video call are not options (e.g. has limited internet bandwidth or travel limitations, has a disability or is Deaf, lives with an abuser and urgently needs support)
- Some survivors prefer this medium
- Connect with younger survivors
- For check-ins and emotional support between sessions for current clients
- An option for friends and family to gather information for a survivor

What an encrypted chat application looks like

- Servers are located in Canada (or Europe) or at least data is inaccessible to vendor
- Designed for the GBV, non-profit or health sectors, not for the private sector
- Web-based; end-users are not required to have an account
- No passive data saved about users (e.g. IP address)
- End-to-end encryption
- Sessions will time out after a specified time and will auto-delete when ended
- User friendly

Chat applications used by GBV organizations in Ontario

- **Resource Connect**
  - American company, data is inaccessible to vendor
  - Designed for non-profit organizations
  - Web-based, end-to-end encryption, auto-delete and time out features
  - Also offers text, automated language interpretation, client database
- **Safe Support Chat**
  - Ontario developer (Just Chat, Info@JustChat.Tools) with servers in Canada
  - Developed specifically for the Ontario Coalition of Rape Crisis Centres (OCRCC)
  - Web-based, end-to-end encryption, auto-delete and time out features
  - Also offers text and WhatsApp Safe Support Chat

TIP

When using encrypted chat and text applications, web-based chat is more secure than text.

When implementing

- Talk with other agencies that offer a chat service for information and tips
- Provide accessible, easy to understand safety information and terms of use about the chat service for survivors on your organization's website; refer users to this material when seeking informed consent
- Set limits for the conversation and communicate these to service providers and survivors
    - Stick to fact based information
    - Refer survivors to the phone line or an in-person meeting for deeper support and intake requests
    - Prepare policies and standardized messages (you may be able to adapt the policies for your organization's crisis line)
- Test the service for an initial period of time and evaluate next steps
- Have a promotional plan

Support service providers

- Acknowledge and respond to safety and workload concerns
    - Make space for learning and getting comfortable: it will take a bit of time
    - Provide training and guidelines, encourage peer-mentoring
    - Ensure multiple service providers are prepared to provide chat support
    - Provide guidelines on protecting service provider identity
- Ensure service providers have appropriate time in their workday to deliver the service
    - Plan for conversations to take much longer than they do by phone
    - Monitor demand, recognizing that it may ebb and flow
- Service provider well-being
    - Acknowledge that they will receive disclosures (e.g. survivor or children at risk) but likely have limited ability to provide support
    - Set up supports for service providers who receive numerous or graphic written disclosures
    - Provide guidelines on dealing with survivor crises and abusive users
    - Establish regular debriefing time with supervisor and team, space for self-care

Standardized messages

These aid service providers to initiate and manage specific situations as well as follow policy requirements; when appropriate, customizing some messaging will make the exchange more personal

- Welcome
- Risk and consent to use (e.g. “Please read our terms of use [website link] and consent to using this chat by typing YES”)
- Limitations of service (e.g. “I can tell you about our services.”)
- Referral information that can be copied and pasted
  - A listing of relevant local services
  - Where to refer a survivor who is outside your organization’s catchment
- Mandatory reporting when a survivor’s identity is known (e.g. child at risk)

Prepare for misuse: Messaging and processes

- When a user asks about a survivor (e.g. “I don’t have that information.”)
- When a user is impersonating a survivor
- When a user is abusive to a service provider

Email: A Problem With Solutions

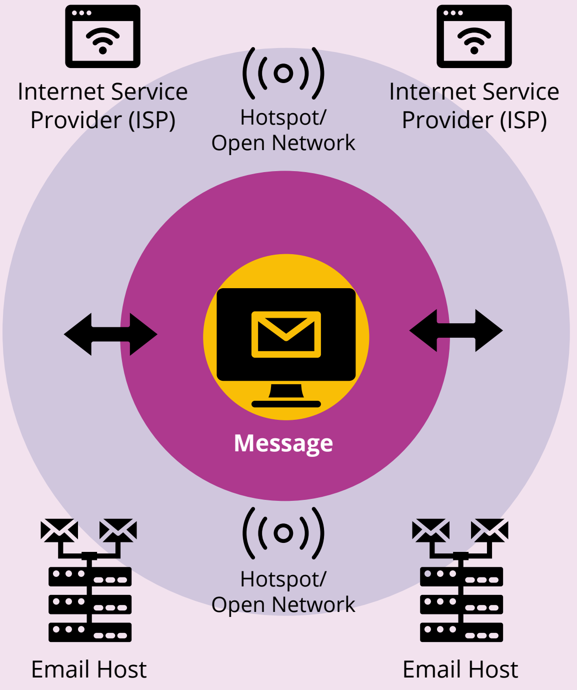
PROBLEM: Email is not a secure way to share personal information

SNAPSHOT OF POSSIBLE ISSUES

SERVICE PROVIDER

Security issues at work:

- Abuser may subpoena emails
- Supervisor and tech support will have access to account
- May share account with co-worker
- If working from home, family/roommates may gain access
- Email can be accidentally sent to the wrong person



SURVIVOR

Security issues:

- Abuser may share or hack into email account
- Abuser may know or guess password
- Abuser may install spyware
- Children may access account
- Employer and tech support will have access to work email account
- Email can be accidentally sent to the wrong person

Technological reasons

When an email is sent, there are actually many copies created between the sender and receiver. **Any of these copies could be intercepted by someone**

- Message saved in sender's and receiver's email application (e.g. Outlook) or email host server (e.g. Gmail)
- Deleted message saved in sender or receiver's email application or email host server trash
- Message can be intercepted through the sender or receiver's internet service provider and through shared networks, such as public WiFi or a home office network
- An organization's network backup may have a copy of the message

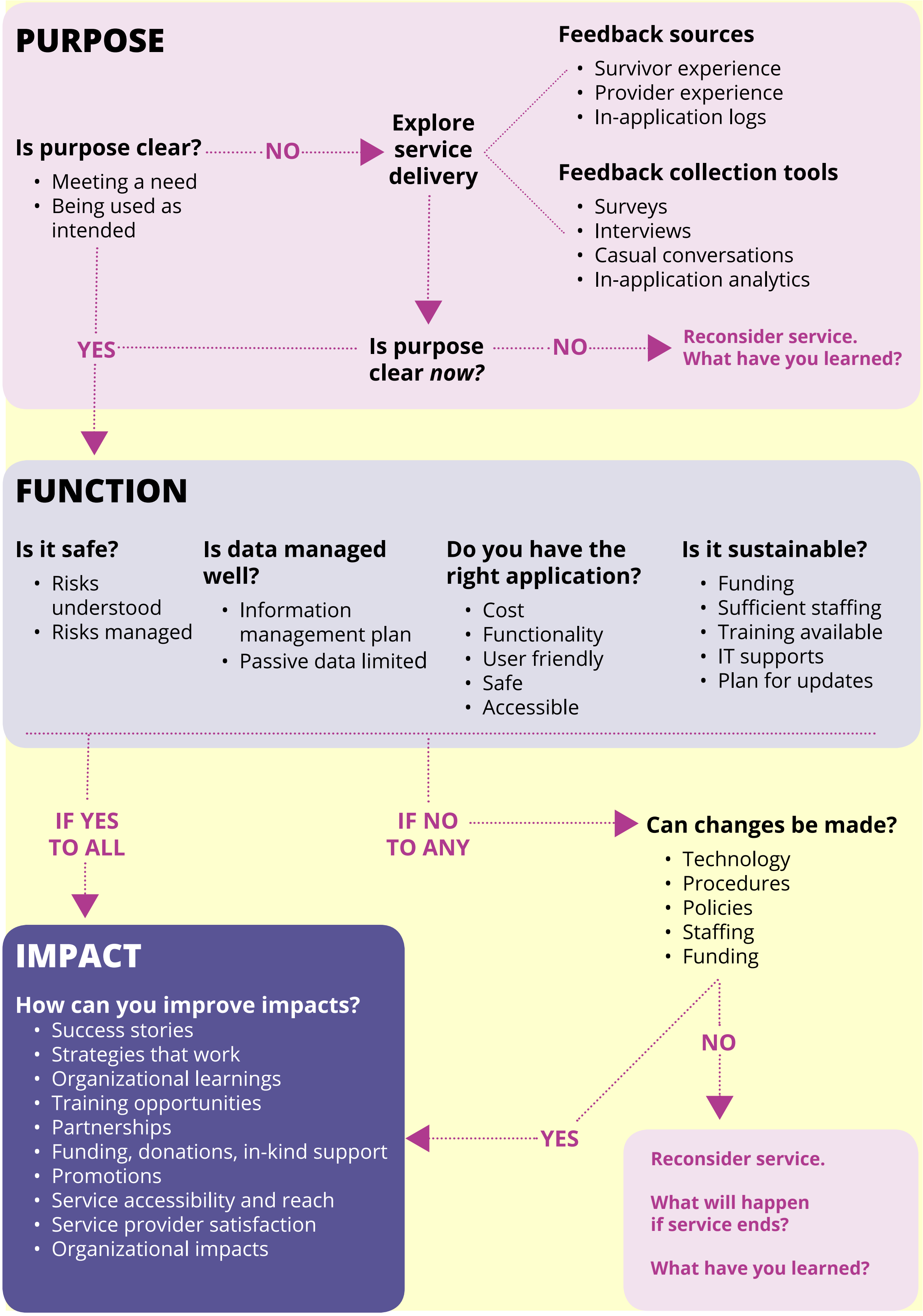
Human factors

- The abuser may
    - Share the email account with the survivor
    - Know or guess the survivor's email password
    - Have installed spyware on the survivor's device
    - Impersonate the survivor using the survivor's account
    - Subpoena all data related to the survivor from your organization if the couple is involved in the courts
- The survivor's children, friends or others may have access to the email account
- Emails can easily be accidently sent to the wrong person and forwarded
- People in your organization may have access to your computer or email account, for example, IT support

SOLUTIONS

- Use more secure options instead (e.g. phone calls, encrypted chat, video calling)
- Explain the risks for email and discuss options with the survivor
- If email is used
    - Have the client set up another account that the abuser cannot access
    - Have the client access their email from a device the abuser cannot access (e.g. a library computer, a friend's phone or a workplace device)
    - Make the subject line vague
    - Before sending a message ask yourself, "What if the abusive person saw this?"
    - Avoid email threads; begin each message as a new email
    - Use code words for critical topics
    - Have and follow an organizational policy for deleting emails
- Do not share client information in email with colleagues

Virtual Service Assessment



PURPOSE

Is purpose clear? NO → **Explore service delivery**

- Meeting a need
- Being used as intended

Feedback sources

- Survivor experience
- Provider experience
- In-application logs

Feedback collection tools

- Surveys
- Interviews
- Casual conversations
- In-application analytics

Is purpose clear *now?* NO → **Reconsider service. What have you learned?**

YES

FUNCTION

Is it safe?

- Risks understood
- Risks managed

Is data managed well?

- Information management plan
- Passive data limited

Do you have the right application?

- Cost
- Functionality
- User friendly
- Safe
- Accessible

Is it sustainable?

- Funding
- Sufficient staffing
- Training available
- IT supports
- Plan for updates

IF YES TO ALL

IF NO TO ANY → **Can changes be made?**

- Technology
- Procedures
- Policies
- Staffing
- Funding

NO

Reconsider service.

What will happen if service ends?

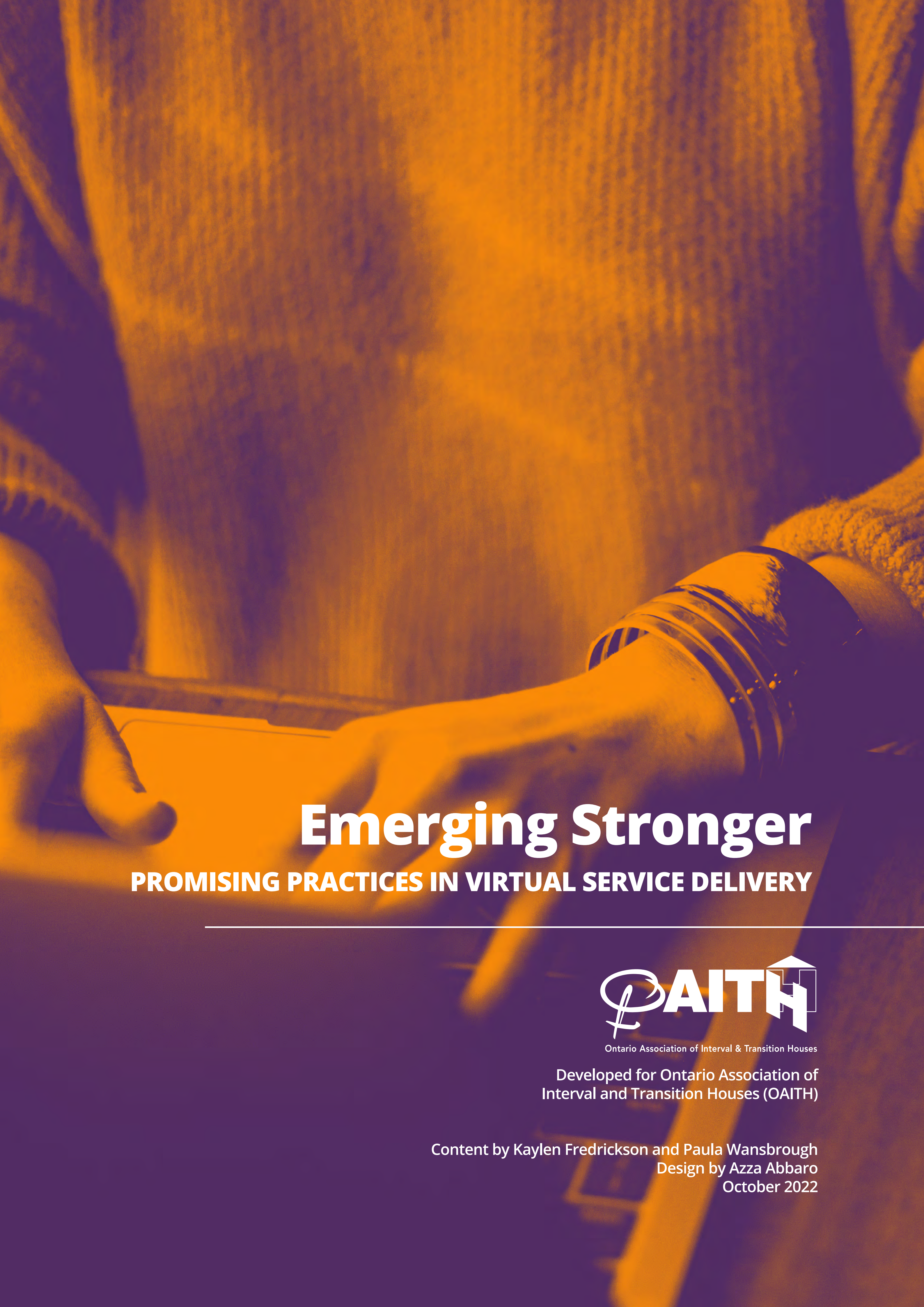
What have you learned?

YES

IMPACT

How can you improve impacts?

- Success stories
- Strategies that work
- Organizational learnings
- Training opportunities
- Partnerships
- Funding, donations, in-kind support
- Promotions
- Service accessibility and reach
- Service provider satisfaction
- Organizational impacts



Emerging Stronger

PROMISING PRACTICES IN 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