Anti-Violence Organization Template: Informed Consent for Digital Support Services

Background

<ORGANIZATION NAME> will be using digital services to provide <type of support> to women, children, and youth experiencing domestic violence. Digital support services, unlike face-to-face services, use third-party platforms to facilitate support sessions.

<INSERT ORGANIZATION NAME> is offering digital support services and this informed consent form covers these services only. This form is an addendum to the <ORGANIZATION NAME> informed consent form you already signed.

This form provides information to you about the third-party digital service provider(s) our organization is using to provide digital support services. Your informed consent is required by the <name of privacy act> before you access the <ORGANIZATION NAME> support in person or by digital support services.

<ORGANIZATION NAME> complies with <name of privacy act>, which creates and enforces rules about collecting, using, and disclosing the personal information of survivors.

Digital Support Services Technology

<ORGANIZATION NAME> provides <type of support> through the following third-party vendors: (Include all digital services offered by your organization)

- ☐ Phone <insert mobile or landline device, e.g. Telus Mobility>
- ☐ Email <insert product or vendor name, e.g. Shaw Communications>
- ☐ Text Messaging <insert organization-owned or employee-owned device, e.g. Rogers Wireless>
- ☐ Real-Time Web Chat <insert product name or vendor name, e.g. Resource Connect>
- ☐ Webcam/Video Conferencing <insert product name or vendor name and plan, e.g. Zoom or Resource Connect>
- ☐ Apps <insert product name or vendor name, e.g. WhatsApp>
- ☐ Social Media <insert product name, e.g. Facetime>

Organization Security Measures

<ORGANIZATION NAME> acknowledges that by communicating through third-party vendors' digital platforms, there may be risks to survivors' privacy. Any digital communication is not guaranteed to be secure or private.

<ORGANIZATION NAME> has implemented security measures to reduce security risks including interception of information, impersonation of the survivor, and breaches of privacy:

<Adapt the list below to include the security measures your organization has in place. See the list below for some examples>

Devices:

- ☐ Laptops, computers, tablets, and smartphones are owned by <ORGANIZATION NAME> and are used for work purposes only
- ☐ Laptops, computers, tablets, and smartphones are password-protected
- ☐ Anti-virus software is installed on all of our devices
- ☐ Anti-malware software is installed on all of our devices
- ☐ Organization staff are required to regularly update device software when new versions are available
- ☐ <ORGANIZATION NAME>'s privacy policies require staff not to store participant names, phone numbers, and emails on our devices
- ☐ <ORGANIZATION NAME> requires devices to be set to not back up conversations and contacts to cloud storage

Accounts:

- ☐ Organization staff communicate on <the third-party vendor platform> through an organization account
- ☐ Organization-owned accounts are password protected

Third-Party Vendors:

- ☐ <ORGANIZATION NAME> has read the Privacy Policy of <the third-party vendor>
- ☐ <ORGANIZATION NAME> has selected <name of third-party vendor> , which incorporates end-to-end encryption of communications

Collection of Personal Information by Third-Party Vendors

<ORGANIZATION NAME> acknowledges that by communicating through third-party vendors' digital platforms, there may be risks to survivors' privacy related to the third-party vendor's practices.

Some of these practices include:
<Adapt the list below to reflect the third-party vendor privacy policy statements>

- The <third-party vendor> collects personal information such as name, email address, phone number, and address when you create an account to use the platform
- The <third-party vendor> collects incidental personal information when you download the app or organization version of their platform such as IP address, general location, and/or device information
- The <third-party vendor> requires an email address for participants to begin digital service provision, which is collected and stored by the them
- The <third-party vendor> collects the following personal information: <list>
- The <third-party vendor> stores the following personal information on their servers: <list>
- The <third-party vendor> has access to the following personal information: <list>, for the purpose of: <list>
- The <third-party vendor> sells, trades, and shares the following personal information: <list>
- The <third-party vendor> will email you promotional material
- By signing into the <third-party vendor> with your social media or Google account, you may be granting permission for the platform to share and access your personal information

Organization Responsibilities:

- While providing digital support services, organization staff will plan to be alone in a private room that is free from distractions or third-party presence
- Organization staff and the <ORGANIZATION NAME> have implemented security measures to reduce risks such as interception of information, impersonation of the survivor, and breaches to privacy
- Organization staff will maintain and continue to take notes of the digital support services session and will include them in the existing participant file. These notes will not be taken, uploaded, or stored on the <third-party vendor platform>.

Participant's Responsibilities for Digital Support Services:

<ORGANIZATION NAME>'s digital support services involve communicating with you or your minor child through your own mobile devices or technology.

The security of your own devices is important to protecting your privacy. If you are uncertain of the security of your own devices or if you suspect that your device is being monitored, please advise the <ORGANIZATION NAME> staff so we can support you with technology safety planning to determine if digital support services are appropriate for you.

Informed Consent to Digital Support Services

In addition to the informed consent form already signed and provided to <ORGANIZATION NAME> for support, I have read this Informed Consent to Digital Support Services and agree that:

- ☐ I understand that <ORGANIZATION NAME> cannot guarantee that the personal information provided for the purposes of digital support services through <third-party vendor name(s)> will not be intercepted.

- ☐ I understand that there are privacy risks (listed above) associated with engaging in support services through <third-party vendor name(s)>.

- ☐ I understand that I am responsible for the security of my own devices used for support services.

- ☐ I understand that the following requirements are needed in order to access support services through <third-party vendor name(s) and adapt to platform>:
    - Access to a mobile device
    - Internet access
    - Access to a vendor account
    - Ability to download an app if necessary
    - And any other specifications: <add third-party vendor specifications>

- ☐ I understand the information obtained through the <ORGANIZATION NAME>'s digital support services may still be subject to disclosure in the following limited circumstances:
    - If staff have reason to believe that a child needs protection, they are obligated (as are the general public) to inform the <government organization> as per <child protection act>
    - If staff have reason to believe that I or my child is likely to cause serious physical harm to myself/themselves or another, they are obligated to inform the appropriate authorities
    - If staff are required by court order to disclose specific records or to testify in court

- ☐ I understand that to help maintain the privacy of my remote support service, I will do my best to consider the following for myself and/or for my child:
  - Participating in my session in a private space or using headphones to increase the privacy of the session
  - Using password-protected online connections and Wi-Fi network
  - Refraining from the use of social media accounts such as Facebook, etc., to sign in to <third-party vendor platform> as they may not be secure
  - Keeping all meeting invitations, passwords, and links to access sessions secure to the best of my ability

- ☐ I consent to having <ORGANIZATION NAME> staff provide digital support services and in doing so to collect personally identifiable information for the purpose of services via <third-party vendor platform> to me and/or my minor child.

The digital support services at <ORGANIZATION NAME> are voluntary. As such, this consent form expires on this date: _____.

I understand that by signing, this I am agreeing to <ORGANIZATION NAME>'s digital support services through third-party vendors and that I may withdraw my consent **at any time** either orally or in writing.

Survivor's Name (print): _____

Parent/Guardian's Name if applicable (print): _____

Signature of Parent/Guardian: _____

Date: _____

Signature of Counsellor: _____

Date: _____

Reaffirmation and Extension (if additional time for digital support services is necessary)

I confirm that this informed consent form is still valid, and I agree to extend my consent until

_____ _____
New Date New Time

Signed: _____ Date: _____ Witness: _____

Adapted for Canada with permission from BCSTH's Technology Safety Project, based on their resource PEACE Organization Informed Consent for Digital Support Services Template.

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

Women and Gender Equality Canada | Femmes et Égalité des genres Canada