Use of personal social media accounts — appropriate conduct

This policy does not intend to inhibit personal use of social media but instead flags up those areas in which conflicts might arise. [*Charity name*] staff are expected to behave appropriately, and in ways that are consistent with [*charity name*]'s values and policies, both online and in real life.

1. Be aware that any information you make public could affect how people perceive [*charity* *name*]. You must make it clear when you are speaking for yourself and not on behalf of [*charity name*]. If you are using your personal social media accounts to promote and talk about [*charity* *name*]'s work, you must use a disclaimer such as: "The views expressed on this site are my own and don't necessarily represent [*charity name*]'s positions, policies or opinions."

4. Use common sense and good judgement. Be aware of your association with [*charity* *name*] and ensure your profile and related content is consistent with how you wish to present yourself to the [*general public, colleagues, partners and funders (delete as* *appropriate)*].

10. Always protect yourself and the charity. Be careful with your privacy online and be cautious when sharing personal information. What you publish is widely accessible and will be around for a long time, so do consider the content carefully.

11. Think about your reputation as well as the charity's. Express your opinions and deal with differences of opinion respectfully. Don't insult people or treat them badly. Passionate discussions and debates are fine, but you should always be respectful of others and their opinions. Be polite and the first to correct your own mistakes.

12. We encourage board members to share tweets and posts that we have issued.

* Be cautious – think before you post. Is this something that you do not mind seeing on the front page of the newspaper? Post responsibly.
* Do not share information that [Charity name] has contractually agreed to keep confidential, for example, proprietary information, trade secrets, and security information.  Think before sharing legally protected privileged information, such as attorney-client, physician-patient, and other privileged information recognized by a court.
* Be aware that social media sites are not the place for a private conversation. Face-to-face meetings or telephone conversations may be more appropriate.
* Do not allow anger or other negative emotions to cause you to post information that you will be sorry for later. Is this something that you would be ashamed of if you read it months, or years from now?  Remember that what you place on social media sites, and in e-mails, text messages, and chat rooms can spread quickly and permanently remain on the internet or in someone’s possession. Statements that are harassing, discriminatory, defamatory, and terroristic are not suitable and could subject board members to a legal action. Be polite.
* Do not use abusive, profane, threatening, or offensive language. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
* Do not conduct board business on social media sites.  Instead, use these sites for listening or reading about others’ opinions, making announcements, having conversations, and obtaining feedback.
* Comply with the law and relevant policies.
* Never post pictures, videos, or other information about specific survivors or any incidents that are not public knowledge as this may reveal the identity of survivors and violate confidentiality.
* Be strategic when posting information about private events, such as support groups or non-public events. This information may inadvertently inform abusers or stalkers where victims will be or invite opposing groups to crash private events.

Because of the safety and privacy risks to women and youth, we recommend agencies:

• Do not post personally identifying information (name, photos, videos) about staff, colleagues, financial supporters or people who attend an event you host unless your agency has informed consent.

 • Do not disclose or share a survivor’s personally identifying information. • Do not disclose or share any information about a survivor’s case or situation.

• Avoid soliciting information or conducting counseling about abuse using social networks.

• Facilitate regular in-person sessions where VAW program participants/residents can discuss and learn about social media privacy and safety issues.

• Don't assume that the visible social media identity is accurate. Survivors sometimes use pseudonyms, and perpetrators sometimes impersonate survivors and others. Remember that perpetrators of technology-enabled domestic violence, sexual assault, stalking, harassment and abuse regularly change their tactics in an attempt to maintain power and control. Social media is just one of many tools they will use to be abusive. Given this reality, the safety and privacy strategies a woman or youth tries will likely vary and evolve.

• For many women, data privacy and confidentiality are critical to their efforts to protect their children, pets and other loved ones, and to stay safe and alive.

• Some women who are being stalked, harassed and abused in person and via technology, speak publically about the abuse because they believe this is the strategy that will best keep them, and often their children, safe and alive.

* When responding to questions or comments, solicit input from staff “issue experts.”
* Have a clear disclaimer on all platforms that indicates where survivors can find support.