Privacy, Security and Confidentiality: Social Media Considerations for Violence Against Women Programs

Safety Net Canada 2013

SAFETY NET CANADA

SAFETY NET CANADA

Safety Net Canada is a national initiative of the British Columbia Society of Transition Houses and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Safety Net Canada addresses how technology impacts and can enhance safety, privacy, accessibility, autonomy, justice and human rights for women, youth and other survivors of family and domestic violence, sexual and dating violence, stalking, harassment and abuse.

Safety Net Canada est une initiative nationale de la Colombie-Britannique Society des Maisons de Transition (BCSTH) et la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC). Safety Net Canada étudie l'impact de la technologie et la façon d'accroitre la sécurité, la confidentialité, l'accessibilité, l'autonomie, la justice et les droits de l'homme à l'égard des femmes, des jeunes, des enfants et des victimes de violence familiale et conjugale, de violence sexuelle, de harcèlement et d'abus.

CONTRIBUTIONS BY

Research, Writing, Editing:	*Cynthia Fraser* *Rhiannon Wong*
Graphic Design:	*Hannah Lee*

PERMISSIONS

FINANCIAL

This project has been funded by the Office of the Privacy Commissioner of Canada. The views and opinions expressed herein are those of BCSTH and CIPPIC and do not necessarily reflect those of the OPC.

In-kind contributions to this work by BCSTH, CIPPIC, the U.S. National Network to End Domestic Violence (NNEDV), and Safety Net Canada's founder Cynthia Fraser.

BC Society of Transition Houses

cippic

SAFETY NET CANADA

NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE

TABLE OF CONTENTS

1. INTRODUCTION

Social media is used by violence against women programs (VAW programs[1]) for many reasons. Anti-violence agencies organize online activities to empower women and youth, support the voices of survivors, engage the community in preventing and ending violence, and honour the women and children who have died as a result of gender-based violence. Social media can exponentially broaden who your agency engages with and learns from. Social media platforms enable VAW programs to quickly collaborate, learn about, share information, and develop more nuanced responses to issues impacting survivors. This is particularly relevant when perpetrators misuse social media to invade their privacy and threaten their safety.

VAW programs know we must plan our social media activities strategically to best support autonomy,[2] safety and confidentiality without unintentionally increasing risks or harm. In technology-enabled campaigns, participants might be asked to sign an online petition, make a financial donation, upload photos of themselves with campaign messages, post on social media sites, make and post videos, text campaign messages to others, tweet about experiences of abuse, or, otherwise use technology to engage others. All of these activities may have identifiable privacy and safety risks for some women and youth who are fleeing and/or living with the effects of sexual violence, domestic violence, harassment, stalking and other forms of violence against women.

Canadian VAW programs play a pivotal role in enhancing survivor safety and changing social norms and behaviours that underpin gender-based violence. Many VAW programs provide violence prevention, education and skills building activities for schools, businesses, government and community groups. Some of these agencies have even created innovative online apps,[3]-[4]-[5]

[1] VAW programs come in many forms. Examples include women's shelters, transition and interval houses, rape crisis and sexual assault centres, children who witness abuse programs, crisis/helplines and more. We know the word "program" also commonly refers to a computer program (or set of code that makes something happen). While computer programming language is used in all social media applications, to avoid confusion, this guide talks about social media applications or platforms, services, settings and features. Throughout this piece, the word "program" refers to the umbrella term "VAW programs."

[2] Autonomy involves the freedom to make choices and determine one's own actions. Agencies can support autonomy by providing meaningful information about the potential risks and benefits of interacting with your agency's social media activities and spaces.

[3] Metrac. "Not Your Baby." iPhone app addresses sexual harassment. Retrieved at: http://metrac.org and http://itunes.apple.com/us/app/not-your-baby/id545191859?mt=8. Toronto, Ontario: Canada.

[4] YWCA Canada. (2010, 2012) "Safety Siren." Smartphone app sends emergency alerts, sounds alarm, has resources. Toronto, Ontario: Canada. Retrieved at: http://ywcacanada.ca/en/pages/mall/apps.

[5] Securiguard."SOS Response." Smartphone app's alarm sends location and photos to a 24/7 monitored service that dispatches local authorities. Available at: http://sos-response.com/eva. Vancouver, B.C.: Canada.

videos, quizzes and games[6]-[7] to engage women and girls, as well as boys and men, in interrupting and preventing gender-based violence.
When engaging in public outreach via technology, it is important to regularly assess the capacity of your agency and VAW program and the potential impact on privacy, confidentiality and safety. Designed well and staffed sufficiently, your social media presence and activities can engage and motivate Canadians to take an active role in challenging and preventing violence against women and youth, including culturally motivated violence. At a minimum, VAW programs can model ways that interrupt victim-blaming and support survivors' rights and needs by strategically speaking up in trending[8] social media discussions.

This guide will assist VAW programs to assess their needs and capacity to use social media; it will help agencies examine their readiness to use social media in ways that minimizes risks and maximize benefits for agencies, survivors and the public. This process will support VAW programs to develop social media practices and policies that respect confidentiality, protect privacy, increase safety and enhance autonomy.

[6] Metropolitan Action Committee on Violence Against Women and Children (Metrac). "What It Is. A digital game Challenging Sexual Violence." for age 12-15 and "RePlay: Finding Zoe/ReJouer: Où est Zoé?" an online game on healthy relationships, for age 8-14. Toronto, Ontario: Canada. Available at http://metrac.org/replay/index.html and http://challengesexualviolence.ca.

[7] Action ontarienne contre la violence faite aux femmes; Ontario Coalition of Rape Crisis Centres. Draw the Line (sexual violence prevention campaign). Traçons-les-limites (une campagne de prévention de la violence à caractère sexuel) Ontario: Canada. Available at: http://draw-the-line.ca and http://tracons-les-limites.ca

[8] "Trending" is a term that identifies the most popular topics currently being discussed on social media.

2. ASSESS CAPACITY AND READINESS

Before deciding to use a social media platform, it is important for your agency or program to identify your:

- Goals, Values, Activities
- Audience or Participants
- Available Tools
- Agency and VAW Program Capacity
- Staffing Capacity and Readiness
- Training Needs
- Costs
- Communications Plan
- Website Integration

Canadian VAW programs are using social media to:

Engage and mobilize the public.
Ignite social change.
Broaden social awareness.
Influence the digital discourse.
Challenge disparities in digital worlds.[9]

In our 2013 Organizational Technology Practices Survey,[9] Canadian VAW programs said their broad goals for using social media are to: engage and mobilize the public; ignite social change; broaden social awareness; influence the digital discourse; and challenge disparities in digital worlds.

[9] Safety Net Canada. (2013) Summary Report: Organizational Technology Practices Survey of Canadian Violence Against Women Programs, 2013. BCSTH. Vancouver, B.C.: Canada.

2.1 Goals, Values, Objectives and Activities

GOAL

- Why does your agency or program want to use social media platforms?
- What are you trying to accomplish? What is your desired result or goal?

VALUES

- Does your proposed social media goal fit with your agency's mission/vision and values? Describe how it fits.
- How will you embody your VAW program's values when using social media[10]?
  - For example, in social media, what does it mean to be listening, believing, actively influencing, providing strategic support or being a thought-leader? What does it mean to be trustworthy, women-centred or to value safety?
- Identify values that match behaviors, and, behaviors that match values:
  - List your core values. Then, figure out how each value translates into ways you might or would not use social media.[11]
  - How will you provide upfront and ongoing notice about privacy and safety issues relevant to the proposed social media channel, action or campaign? How does this activity embody your values?

OBJECTIVES

Objectives identify who does what, where, when and how. They are SMART: Simple/specific, Measurable, Attainable/achievable, Realistic/relevant, Time-framed.[12]-[13]

- What concrete measurable objectives will achieve your social media goal?
  - For example: *by [timeframe], [who] will disseminate our social media campaign privacy and safety tips a total of [#] times via [#] social media platforms [for example, Twitter, Facebook, Google+] to [#] site/feed followers/visitors/participants.*

[10] Idealware. (2012) Nonprofit Social Media Policy Workbook. Page 11. Portland, ME: USA. Available at: http://www.idealware.org/reports/nonprofit-social-media-policy-workbook

[11] Idealware. (2012) Nonprofit Social Media Policy Workbook. Page 11. Portland, ME: USA. Available at: http://www.idealware.org/reports/nonprofit-social-media-policy-workbook

[12] Idealware. (2011) Nonprofit Social Media Decision Guide. Page 11. Portland, ME: USA. Available at: http://www.idealware.org/reports/nonprofit-social-media-decision-guide

[13] Idealware. (2013). Exploring Cutting Edge Social Media. Page 6-7. Portland, ME: USA. Available at: http://www.idealware.org/reports/cutting-edge-social-media

ACTIVITIES

What activities are needed to achieve each objective? Be specific. For example, will you decide to:

- *Identify how the social media features you want to use might increase or decrease accessibility, safety, confidentiality or privacy. Do some features disproportionately impact specific populations? How will you address those barriers or risks?*
- *Identify potential ways for individuals to participate anonymously or using pseudonyms. Which anonymous options best enhance safety and privacy for survivors?*[14] *What are risks of perpetrator misuse?*
- *Create tips about safety and privacy issues that might arise for some survivors. Disseminate tips as part of all campaign material and outreach, including on your website, listserv and other social media feeds. During the campaign/action, repost tips several times a day to the primary social media page/feed for the campaign/action.*
- *Identify three safety tips related to [social media site's] privacy settings. Share them five times before and five times during, and three times after a 75 minute online chat you host on [social media site].*

- What support will you need to implement these activities?
  - Brainstorm an initial list. Identify people or resources that might help. More support needs will arise as you engage further with social media.

2.2 Audience/Participants

Different age and cultural groups use different social media/network applications and sites. Assess benefits of using various social networks/media (for example Facebook, Twitter, MySpace, Instagram) based on how it will engage and involve the people you want to reach.

- Whom do you want to reach?
- What are their needs?
- How do you want to involve these participants online and offline?

[14] Mumsnet.com. (2012 March) "We believe You." Rape Awareness campaign was launched in March 2012 to raise awareness about why sexual assault survivors did not go to the police or others to report that a crime had been committed against them. People began to tweet to hashtags #ididnotreport, #ididreport and #ibelieveher. Privacy is a critical concern for many survivors of sexual assault. The campaign organizers created Twitter accounts (@ididnotreport1 at http://twitter.com/Ididnotreport1) and regularly tweeted the account user name and password. They did this so that sexual assault survivors could share their experiences anonymously. By owning the @ididnotreport1 account, organizers retained the ability to delete problematic or harassing posts. The anonymous account option increased accessibility, safety, privacy and thus participation; it was used both by people without Twitter accounts, and by people with Twitter accounts who were more comfortable sharing experiences anonymously.

Learn what matters to your audiences in a social media platform.

- What is a social media site's reputation with these audiences?
- What policies does a social media site have, to address the safety, privacy and other needs of your desired participants?
- What's the site's track record? If harassment or violations have been reported, how were they addressed?
- Which social networks does your desired audience use and why?

Features and policies of social media/networks evolve regularly. These changes can affect the safety, privacy and accessibility needs of the people you want to reach and engage, especially if they are abuse survivors.

- Where are the people you want to engage, most active? Have they moved to other social media platforms? If so, why?
- Periodically evaluate your social media for its continued fit.

2.3 Considering Social Media Tools and Features

There are a variety of social media applications available from blogs, social networks, photo sharing and more! It's okay to work in phases and take on one social media application or feature at a time.

Start with what you know. Brainstorm**.**

- What social media and networks are you aware of?
- What is your current staff using?
- What are current VAW program participants/residents using?
- What is your target audience/demographic using?
- What features do folks like and why?
- What features are you looking for?
- What do you want to know more about?

Learn how other nonprofit agencies are engaging in social media. **Use the resources listed at the end of this guide.** They are developed by organizations that already track, assess and create guidance on social media tools for nonprofits and/or VAW programs.

- For example, Idealware's Nonprofit Social Media Decision Guide addresses common tools to consider using; Exploring Cutting Edge Social Media offers guidance on less-familiar tools, and their Nonprofit Social Media Policy Workbook helps agencies develop policies to fit your values and culture.

Get specific about your needs. Narrow down your choices.

- What core features and settings do various social media platforms offer, that you might use to achieve your objectives and goals?
    - For example, do settings let you review posts from visitors before they show up on your public wall/channel? Can you disable the option for visitors to send you private messages?
    - What are the safety and privacy implications of changing settings?
- When you access the social media channel via different devices (for example, a computer versus a mobile phone) do core functions differ?
    - What if you access it via a Web browser versus an app? Or, an Android versus an iPhone? Will device access cause barriers for key participants you want to involve in your social media channel?
- What options and supports does the platform have for nonprofit organizations?
    - Does the platform make it easy for designated agency staff to have professional profiles/accounts? Can the professional accounts be distinct or would they need to be linked somehow to a personal profile/account?

Because social media keeps changing, consider the evolution, lifecycles and reputation of the social network or media platform.

- How well does the social media platform implement changes and upgrades?
- Do they design sufficient privacy and security options into their technology?
- How transparent are they when they change settings, policies or practices that can and will impact the safety, privacy and security of survivors?
- How do they respond to reported policy violations that involve gender-based violence or abuse? What is the culture of the site?

2.4 Agency and VAW Program Capacity

- What time commitment can your agency and VAW program make to specific social media activities?
- Which platforms will be easier or harder for your agency to use?
- What devices or equipment might your agency need?
- How will you assess, coordinate, develop, monitor, maintain and update the social media profile, pages and activities you are considering?

2.5 Staffing Capacity and Readiness

- Which social media platform, features and ongoing activities can your agency adequately staff now? In six months? In a year?
  - Can you phase in features to match staff capacity? If you don't have the capacity to respond to comments, consider initially turning off some of the features. Some social media platform settings (for example, Facebook) let you turn on or off options for people to (a) send private messages (b) respond to posts by your agency on your channel or (c) post separate comments on your wall/channel/page.
- Will ongoing social media duties and tasks be spread across several job roles or centralized in one job position?
- Which staff will be responsible for what?
  - Will staff monitor external social media for mentions of your topics or agency name?
- Will your agency provide any equipment needed or will staff also be asked to use personally owned devices?

- Is staff prepared to be contacted by site visitors?
- What boundaries, guidance and support will your agency provide to all staff when addressing social media comments and requests?

Social media issues emerge 24/7 including during evenings, weekends and holidays.

- Will your agency ask or expect any staff to assess or address social media issues during off hours?
- If staff members are asked and able to flex their hours, can your agency proactively identify situations and anticipate support needs?

2.6 Training

- What training will designated staff or volunteers need?
- Since functions and policies of social media platforms evolve regularly, how will you support ongoing training needs? How will staff stay current on things like: the difference between Facebook and Google+ privacy settings, or how to remove geotags from photos and videos before posting them online to YouTube, Instagram, Pinterest or Flickr.
- How will you prepare and support staff in addressing posts and contacts from social media site visitors, especially from women, youth, survivors and abusers?
- How will you continue to train staff to implement policies and practices related to social media?

2.7 Costs

- Does the social media application have a cost?
- What about the staff/volunteer time needed?
- Are training or administrative costs involved?
- Any other costs (for example, graphic design)?

2.8 Policies and Practices

- What policies and practices will you need to adapt or create to best address privacy, security and confidentiality issues on different social networks and media sites?

2.9 Communications Plan

- Does your agency have a communications plan? This might include the type of messages, news articles or campaigns that your agency wants to support or promote. Does your plan address what can be posted to your website?
- Do the events, campaigns and news you might share via social media align with agency mission, values and ethics?

- Communicate about online safety risks, emergency contacts and agency availability.
- How will you alert survivors about key safety and privacy risks? Where will you post a safety alert about the benefits of using safer computers/devices and the risks of computer or mobile device activities being monitored by an abuser using spyware?
- Where will you provide visitors with emergency numbers (with area code), agency contact information (including town, province/territory and country), links to your website, staff availability and hours of operation?

Social media encourages following, liking, posting, linking, tagging and sharing. These are activities that most nonprofits promote once they have a social media channel. However, those activities can increase safety and privacy risks for a survivor who is being stalked or harassed online. VAW agencies need to address this complexity when they encourage or measure social media engagement.

- How will you promote your online presence in ways that encourages active involvement and simultaneously raises risks and cautions against it? Basically, how will you consistently communicate “follow us on social media, except, don’t follow us if X,Y,Z are potential privacy or safety risks for you”?

2.10 Website and Social Media Integration

Review or create an online communications plan.

- How do the goals and objectives of your website and social media align?
- How will you coordinate website and social media activities? How will you use your website to keep people engaged with your social media channels, and vice versa?
- Who will regularly promote your website news and resources via social media?
- Which social media accounts will you promote on your website? Why? How?
  - Do you want to stream some of your social media posts via your website homepage? If so, which social media accounts do you want to highlight? For example, your most recent tweets, Facebook posts, or YouTube videos?
  - Will your website need design changes to promote your new social media activities? Include these in your costs.

3. Address Legal and Ethical Issues

Anti-violence agencies and VAW programs need to periodically evaluate their ethical and legal obligations in the context of social media. Your agency may need to seek legal clarification on issues impacted by social media. For example:

- How statutory, regulatory or contractual obligations apply to social media.
- Jurisdictional issues (for example, around supporting survivors and mandatory reports).
- Conflicts of interest (for example, assess if social media relationships impact duty of care).
- Duties of staff who are governed by regulatory bodies[15] based on their professional licensure or certifications (for example, lawyer, counselor, nurse).
- How to address potential mandated reports or respond to subpoenas.
- Identity verification and screening techniques (for example, to thwart a perpetrator who tries to impersonate a survivor on social media).
- Survivors who want or need to use a pseudonym or be anonymous.

Provide clear guidance to staff on all legally sensitive social media issues that raise potential liability for your agency, and/or privacy and safety risks for survivors and staff. If you already have a Statement of Principles[16] or a Code of Ethics,[17]-[18]-[19]-[20] you can use that as a framework to begin analyzing and making decisions about social media and electronic communications. Still, you may need to make updates or provide additional guidance[21] on ethics in a digital age.
The following chart highlights issues, examples and guidance to help you assess social media:

[15] Canadian Counseling and Psychotherapy Association/L'Association Canadiienne de Counseling et de Pyschotherapy. Regulations Across Canada. Available at: http://www.ccpa-accp.ca/en/pathways and http://www.ccpa-accp.ca/fr/pathways .

[16] Ontario Association of Interval and Transition Houses. Statement of Principles. Available at: http://www.oaith.ca/about-us/principles.html

[17] Many VAW programs, social and human service agencies, and licensed professional bodies, create Ethical Codes of Conduct to guide their practice and decision making in unanticipated or complex situations. If your agency doesn't have one, it is good to plan to create one. In the meantime, you can refer to codes created by other VAW programs or related helping professionals for ideas that may fit your agency's values.

[18] BC Society of Transition Houses. Code of Ethics. (1994 June) Available at: http://bcsth.ca/content/code-of-ethics and http://www.ccpa-accp.ca/fr/resources/codeofethics.

[19] Canadian Counseling and Psychotherapy Association/L'Association Canadiienne de Counseling et de Pyschotherapy. Code of Ethics . Code de déontologie. Available at: http://www.ccpa-accp.ca/_documents/CodeofEthics_en_new.pdf

[20] B.C. Association of Clinical Counselors. (2013 June) Code of Ethical Conduct. Vancouver,B.C.: Canada. Available at: http://bc-counsellors.org/general/code-of-ethical-conduct-and-standards-of-clinical-practice and Guidelines for Ethical Decision Making (October 2008). Available at: http://bc-counsellors.org/wp-content/uploads/2011/02/1BCACC-Guideline-Ethical-Decision-Making-2008.pdf.

[21] Sheppard, Glen. Notebook on Ethics, Legal Issues and Standards in Counseling. Available at: http://www.ccpa-accp.ca/en/resources/notebookonethics . It has sections on: "Record Keeping Ideas", Guidelines for Dealing with Subpoenas and Court Orders" and "Ethics, E-mail, and the Counselling Profession."

- Boundaries, Dual Relationships and Conflicts of Interest
  - Between Program Participants and Staff
  - Between Agency and Employees
- Security
- Confidentiality
- Recordkeeping
- Responding to Subpoenas
- Collecting Evidence and Reporting Violations
- Copyright and Terms of Use

3.1 Boundaries, Dual Relationships and Conflicts of Interest

Social Media can blur boundaries between:

- Work roles and private lives.
- Agency and employees.
- VAW program staff and participants.

> "Social Media can blur the boundary between an individual's public and professional lives." [34]
>
> ~British Medical Association worlds.[9]

Some social media site policies require individuals to blur these boundaries in order to do their job tasks related social media. For example, Facebook requires your staff to use their personal account to administrate your organization's Facebook page[22]. Other social media sites (for example, Twitter) do not require people to link personal social media accounts to workplace's social media accounts.

Research how the social media company's policies, platform design and features might impact boundaries and decide how to address:

- Professional licensure or certification (agency and individual)
- Jurisdictional issues (does your funding restrict the geographic regions you serve?)
- Conflicts of interest from dual relationships (If a VAW program employee has a social media relationship/friendship with a woman who contacts the VAW program, what boundaries are in the best interest of the woman/participant and worker?)
- Organizational status and time spent on lobbying[23] activities (would some of your agency's social media posts be considered lobbying?)
- Responding to subpoenas or court orders for agency or employee information

[22] Facebook, Managing a Page. Available at https://www.facebook.com/help/www/364458366957655/

[23] FAQs on Nonprofit Incorporation and Charitable Status. Available at: http://www.corporationcentre.ca/docen/home/faq.asp?id=incnp

3.2 Boundaries Between Program Participants/Residents and Staff

Provide clear guidance to staff so they know what boundaries to set with (former/current) VAW program participants/residents on social media/networks. The agency's social media boundaries should be explained to all program participants and should be grounded in agency values, and legal and ethical obligations (for example, confidentiality). It should be clear that your agency sets these boundaries because it values the safety, privacy and confidentiality of all VAW program employees and participants. Guidelines should be vetted for how they might impact autonomy and self-determination.

- Proactively discuss common situations that can arise when staff and/or current/former participants are using the same social networks.
- What potential risks arise for VAW program staff and/or participants who are already connected via social media?
- What policies will your VAW program develop that ensure the privacy, safety and confidentiality of the women, youth and children your agency supports?
- What policies will your VAW program develop that protect employee privacy, safety and confidentiality?

ANTICIPATE COMPLICATED AGENCY-STAFF-PARTICIPANT BOUNDARY SITUATIONS

Ask VAW program staff who work directly survivors to identify potential scenarios. With each scenario, identify the risks and benefits of potential responses. For example:

- If an employee realizes that on one social media platform, she is the "friend" or "friend-of-friend" of a guy who is stalking a resident at the agency's transition house. The employee is only able to identify the perpetrator on social media because she is privy to confidential information a woman shared with the agency.
  - What safety and privacy planning might be needed?
  - Does the employee now have a potential conflict of interest with the particular survivor, or not?
- Through her personal account, the employee has legitimate access as this social media "friend." Is it solely the employee's decision whether she wants to look at and possibly document the abuser's social media feed/page/posts?
  - What ethical or liability issues arise for your agency in this scenario?
  - What safety and confidentiality issues arise?
  - If the employee wants to change her privacy settings or to block the abusive person from seeing her personal social media page because it makes her feel more safe and private, do changes like that have the potential to somehow alert the perpetrator or/and impact the survivor's safety and confidentiality?
  - In this situation, does the employee have the right to make these decisions unilaterally? Does she have the right to decide based solely on her needs? Or does the agency have expectations that these decisions should be made in consultation with the agency, the survivor or both?
- What sort of guidance will your agency provide staff in these and other scenarios?

3.3 Boundaries Between Agency and Employees

Many employees of non-profit VAW programs already donate personal time and resources to support agency activities and goals. For example, 61 per cent of VAW programs that responded to our 2013 Organizational Technology Practices Survey of Canadian Violence Against Women Programs said their agency work sometimes involved using equipment/devices that are personally owned by staff, volunteers or consultants.[24]

61% of surveyed Canadian Violence Against Women Programs said their VAW program's work does sometimes involve using equipment or devices that are personally owned by staff, volunteers or consultants.[24]

Agencies should not take the generosity of employees for granted. Given the nature of the work to end violence against women, it is essential that agencies respect the personal boundaries and private lives of employees. This includes respecting that employee have certain rights to privacy, whether they are using personally-owned or agency-owned accounts and devices.

"Social Media can blur the boundary between an individual's public and professional lives."[25] How does social media use impact what your agency wants to ask employees to do:

- During work hours?
- In their private lives and non-work hours?
- On agency or personally owned devices?
- On social media sites, apps or platforms?

EMPLOYEES RIGHTS AND AGENCY VALUES

- Do you think your agency has any right to define what staff do or don't do with their personal accounts or personally-owned devices on personal time?
  - What things might your agency ethically expect or ask staff do on personally owned devices or personal social media accounts during work hours?
  - What would be inappropriate, unethical or illegal to ask or require of staff?
- Are your agency's requests or expectations consistent with agency values and obligations staff committed to when they were hired at a VAW program?

[24] Safety Net Canada. (2013) Summary Report: Organizational Technology Practices Survey of Canadian Violence Against Women Programs, 2013. BCSTH. Vancouver, B.C.: Canada.

[25] British Medical Association. (2011) Using Social Media: practical and ethical guidance for doctors and medical students. Page 1. London: UK. http://www.bma.org.uk

BE CLEAR ABOUT WHAT YOUR AGENCY WILL OR WON'T ASK OF STAFF.

Provide clear explanations and guidance for any agency request that involves the personal/private accounts and devices of employees. For example:

- *Our agency will never ask an employee to "friend" colleagues, coworkers, board members, supervisors, funders or program participants on social media sites.*
- *Our agency expects employees not to initiate "friend" requests to current/active VAW program participants via the following social media sites (for example, Facebook). This expectation is consistent with boundaries that VAW program staff have already agreed to set with women and youth who are VAW program participants/residents.*

If your agency expects or encourages an employee to maintain certain social media relationship boundaries with a current/former program participant, you need to provide:

- Realistic guidance on how long you expect the boundary to be maintained[26]
- Clear examples of how your policy does or doesn't apply on specific social media platforms (for example, Google+, Facebook, Twitter, Flickr, Google+, Pinterest, Tumblr); sites such as Facebook and Google+ require the use of a real name, and focus more on personal socializing and relationships; social bookmarking sites like Digg primarily promote articles or content.

Ensure your policy does not somehow create new or unreasonable burdens and privacy intrusions on VAW program staff or participants/residents.

- For example, you do not want staff to think they have to search a social media site for the names of former and current VAW program participants in order to comply with an overly broad, ill-defined or poorly vetted social media policy or practice.

PROVIDE GUIDANCE ON DUAL RELATIONSHIPS AND POTENTIAL CONFLICTS OF INTEREST

What is in the best interests of the VAW program staff and the participant/resident?

- If an employee's friend or social media "friend" asks for help from the VAW program, by default will this be considered a conflict of interest for the employee and the agency?
  - Will this mean the employee can still act in the capacity of a friend, or will other staff provide VAW program support to that participant/resident?
- When are potential conflicts of interest best addressed on a case-by-case basis? In those cases, what must be assessed to decide an appropriate boundary?
- Do you have a Code of Ethics or similar criteria to help staff assess potential conflict of interest related to social media use? For example:

[26] Leaving an abusive spouse or boyfriend can be dangerous and have high safety risks. Fleeing and hiding from a stalker is very difficult in this digital age. Some women or youth will contact a VAW program for support many times over months or years. A VAW program might not hear from a survivor for months at a time, and then the she may show up again needing shelter or safety. Many men who perpetrate domestic violence, dating violence or incest often stalk women and youth for years and even decades. Any guidance around time frames must take this into account.

  - What situations cause potential conflicts of interest to arise?
  - What key questions might an employee ask herself if she is worried about setting the best boundaries for herself and the "friend" seeking help?
- Example of a case-by-case guidance:
  - Agency provides a worksheet with some examples, criteria and questions to consider. Employees must use the worksheet anytime she has dual relationships with a woman seeking services, and needs to assess what boundaries are in the best interests of her and her "friend"; she will also consult one coworker.
  - Agency provides a separate worksheet to help the survivor assess the pros, cons and safety issues that might arise from a dual relationship with a staff person. A different anti-violence worker will explain why the agency assesses conflicts of interests, and sets some boundaries, and will support the survivor in figuring out what boundaries are in her best interests.

These are just a few examples to illustrate that agency guidance can be straightforward, and still provide the flexibility needed to embody your agency's values and vision.

PROVIDE WAYS FOR EMPLOYEES TO EASILY COMMUNICATE WHEN THEIR VIEWS ARE PERSONAL AND DO NOT REPRESENT THE AGENCY

- If staff have a personal blog, website or social media accounts, you might ask them to include a statement that the views they express are their personal opinions and not those of their employer.

Brainstorm a list of potential benefits, risks and concerns if employees:

- List their job on personal social media pages/channels. (for example, Facebook, LinkedIn)
- Post comments about their work day.
- Share and retweet the agency's social media posts.
- Share opinions that are significantly different from the vision, values and ethics of the agency.

DISCUSS PRACTICAL SOLUTIONS AND PROVIDE PRACTICAL GUIDANCE

- Most staff are well-practiced at compartmentalizing their lives and keeping information confidential. Those skills just need to be applied to social media. As a staff, discuss ways folks can post about an "exhausting day" and connect with friends on their personal social media page without compromising anyone's confidentiality.

Develop criteria and guidance to address the safety and privacy implications of more complicated situations, such as:

- When an employee, volunteer, or board member posts views on their personal social media pages that are the opposite of the agency's vision, values or ethics.
- When an employee is social media "friends" or "friends-of-friends" with someone who is being abusive to a woman or youth at the VAW program.

CREATE A GENERAL POLICY, THEN DEVELOP PRACTICES FOR DIFFERENT SOCIAL MEDIA SITES

What social media and location privacy practices and policies do you need to develop or adapt, related to the use of:

- Devices personally owned by staff, consultants, board and volunteers.
- Devices owned by the agency.
- Devices that survivors bring with them such as laptops and mobile phones.

Consult staff:

- Ask staff who are already active on social media sites, to review agency social media policies.
- Staff may have insights on particular social media platforms that the agency hasn't considered; they may know why a policy or practice is not realistic, and be able to suggest practical alternatives.
- Listen especially carefully to staff if they think agency social media requests or expectations are not appropriate.

3.4 Security

Any communication with women, youth, and survivors who contact or access your VAW program should be regarded as highly sensitive and confidential information.

- **Encryption:** Your agency should use encryption whenever confidential information is being communicated, transmitted or stored electronically by your agency. Social media platforms and applications are increasingly using SSL (Secure Socket Layers) to encrypt all their information in transit. Take encryption into account when using social media.
- **Security Settings:** Many social media sites offer user privacy and account security settings and notifications including security questions, two-step verification and the ability to regularly change your password. Review these in any social media site your agency or staff use. For example, Facebook offers login notifications, login approvals, heightened security for unrecognized devices, the ability to see all active sessions, and to review tagged posts before they are published to your wall/page.

3.5 Confidentiality

Confidentiality is critical to safety, and encourages help-seeking by women and youth experiencing or fleeing violence. What are your legal obligations to protect the privacy and confidentiality of individuals who contact or interact with the agency or VAW program?

- What federal, provincial or territorial laws, regulations and obligations apply?
- Do obligations change depending upon the professional licensure, certification or regulatory body that applies to an individual staff member? For example, communications between a woman and her lawyer are protected by privilege.
- Do agency and staff confidentiality obligations occur upon initial contact and request for service? Does a private message or public wall posting to your agency's social

media account, legally constitute a contact or request for support?
- Do the privacy and confidentiality obligations apply regardless of whether the woman or youth accesses agency services immediately, or is wait listed or turned away?[27]

- What are your agency's obligations to protect the confidentiality and privacy of current and former program participants/residents? How will these obligations apply to interconnected conversations and postings in social media settings?
- What if survivors ask for support, or share their story, on your agency's social media pages? How will your agency still protect their confidentiality and privacy as best you can?
- What policies do you need to have regarding staff use of technology to best protect the confidentiality of people who contact your VAW program/agency?

TECHNOLOGY USE, LOCATION CONFIDENTIALITY AND PRIVACY

Location-based services, location-sharing features and location-tracking devices (GPS) create new liability risks that must be addressed in agency policies and practices. What does due diligence look like? What are reasonable steps for staff and agencies to take to avoid causing harm? For example, to protect confidentiality locations:

- Location-based features must be used carefully to best protect privacy. Otherwise, by merely carrying their personal cell phone with them to meet with women and accompany them places, they may unintentionally compromise a confidential location or route used to transport survivors between transition houses.
- Staff should strip geotags from all photos and videos before sharing them or posting them on an agency social media site.[28] Staff should also decide whether or not to strip other metadata that is sometimes stored in files, like name of owner/creator.
- Some agencies might ask employees to disable types of social media account settings and location features on their work and personally owned mobile devices during work hours, or when travelling to and from work. For example, staff may be asked to take precautions such as turning off all geotagging before using their lunch break to take a personal photo, or to write a personal Facebook message.

TECHNOLOGY AND CONFIDENTIALITY: AUTOMATED CONTACTS AND SHARING

These are only a few examples to give you a sense of the many ways that social media and other technology settings and features can have unintended consequences, if not reviewed carefully for their impact on confidentiality.

[27] BC Society of Transition Houses. (2013 May) "New report reveals significant daily demand unable to be met by current programs for violence against women in BC." BCSTH. Vancouver, B.C.: Canada. Retrieved at: http://bcsth.ca/press/new-report-reveals-significant-daily-demand-unable-be-met-current-programs-violence-against

[28] Some women's shelter and transition houses keep their location confidential. Additionally, any geotag can disclose an important confidential or private location. Stalkers look for context. A geotagged image or video might disclose the location of a common meeting place, a staff member's home, a youth center or school, or a woman's new workplace or car mechanic.

- **Contact/Address Lists:** Many social media applications encourage users to let them access your phone's or computer's entire contact list in order to alert you to who else is uses that social media tool. If your contact list includes any names and numbers of VAW program participants or staff, sharing it with a social media application may be construed to violate your agency's confidentiality and privacy obligations.

- **Contact Syncs and Merges:** Many services sync[29] your emails and contacts between mobile phones, computers and online storage. Some automatically offer to merge several contact lists or add new emails/numbers to a contact list, identify duplicates and conflicting information. This can move a contact between devices and spaces and very quickly.

- **Contacts and Social Media Merges**: For example, Google grows your Google+ Circles from your existing Gmail account and contacts[30]. Google automatically suggests additions to Google+ Circles based on your Gmail addresses and contacts. Unless you change some settings, Gmail automatically enables the Gmail users you frequently email to see you, and to chat without having to send an invitation.[31]
    - What if a survivor's phone number or email address is on an employee's mobile phone, but somehow gets automatically synced to the employee's computer, online email and contact list (for example, Google Contact Manager[32] and Gmail, or a global contact list)? For example, in Google, a Gmail box might automatically suggest to a survivor that she add an employee to her Circles.[33] Automated sync settings like these have the potential to compromise the survivor's confidentiality. Your agency needs to assess and address the confidentiality, liability and safety risks of circumstances such as this.

- **Social Media "Friends," "Circles" and Automated Pushes:** Most social networking sites make money from advertising. To do this, they need ways to search for, or share, information about you and the people you connect with. For example, unless you disable the features, Facebook has a setting to let "People Bring Your Info to Apps They Use" and to create "Instant Personalization of Partner Websites" using your (and your "friends") information.

The above examples illustrate why it is important for VAW programs and social media companies to proactively design privacy protections into their technology practices. A little

[29] Google. Google Sync. Sync your Google services to your phone, tablet and desktop programs so that you can always access what is important to you. Available at: http://www.google.com/sync

[30] Google. (2011 December) Gmail and Contacts get better with Google+. Grow your circles from your email. Available at: http://googleblog.blogspot.com/2011/12/gmail-and-contacts-get-better-with.html

[31] Google. (2003) Gmail will automatically invite some contacts. Available at: https://support.google.com/chat/answer/29795?

[32] Google. Google Contact Manager. Available at: https://support.google.com/mail/answer/77259

[33] Additionally, since, you don't need a person's permission to add them to your Google+ Circles, a survivor might unilaterally add an employee/agency or vice versa.

forethought can make a big difference to the safety and confidentiality of a woman or child living with or fleeing technology-enabled abuse and other violence.

3.6 Responding to Subpoenas

Anticipate and have a written response protocol for how your agency will respond if lawyers attempt to access:

- The agency's social media account/s.
- Employee's social media account/s.
- Device/s that the employee used to access either account.

This is very important, if employees must use their personal social media account in order to access and administer the agency's social media page and account. Communicate this protocol to any employees responsible for staffing your social media presence.

3.7 Record Keeping and Communications

VAW programs know that it is not uncommon for some women and youth to ask for information, but not to disclose they are currently experiencing abuse or violence. Given the heightened privacy, confidentiality and safety risks faced by women and youth experiencing or at risk for technology-enabled violence, VAW agencies should treat all electronic communications sent to their social media accounts from women, youth or self-identified survivors as highly sensitive data.

> "Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both. Consent must be invoked in the collection, use and disclosure of one's personal information. Consent must be informed and uncoerced, and may be revoked at a later date."
>
> ~Ann Cavourkian, Information and Privacy Commissioner of Ontario

- Retain the messages in the social media account for the absolute minimum time necessary.
- Restrict access to the fewest staff necessary.
- Protect agency social media communications and any agency records about social media contacts or requests with the strongest available security protocols.
- Use all appropriate legal means and security mechanisms to prevent agency disclosure of confidential information.
- Regularly review and delete information once it is no longer accurate or needed.[34]

RECORD KEEPING SHOULD ENHANCE (AND NOT UNDERMINE) SAFETY, PRIVACY AND CONFIDENTIALITY

- Ethically, VAW programs should not collect, transmit or store sensitive information using technology or other methods that have known security risks, which thus potentially increase safety risks for participants, residents or others who contact the VAW program.

- VAW programs should have default practices and protocols for routinely addressing and deleting communications they receive, and which are temporarily stored in social media accounts.
- The only exceptions are if your agency assesses that you should temporarily keep the electronic communications in the social media account:
  - For evidentiary or legal reasons.
  - Because the person who contacted you via social media has asked the agency to keep her messages for a while, and you have done safety and privacy planning about the risks.

[34] An agency might need to retain information in order to best support the woman /youth/survivor, or for evidentiary or legal or regulatory reasons.

NEVER DOCUMENT ELECTRONIC COMMUNICATIONS USING METHODS THAT MIGHT INCREASE SAFETY OR PRIVACY RISKS FOR SURVIVORS

If an agency communicates with a VAW program participant via social media or other electronic means, it has to assess the safest and most private way to document that communication. VAW programs and agencies must analyse a number of privacy laws and regulations when assessing best practices for keeping agency records about social media, and the accompanying electronic communications.

Any decisions to retain or delete information should be consistent with Canadian privacy values, including informed consent, confidentiality, privacy and a woman's right to control her own information. In addition, record keeping should be informed by the safety and privacy practices that have been developed by those with significant expertise and experience working to end violence against women.

- Any collection or retention of personally identifiable data should be of clear benefit to the woman / program participant the agency is supporting.
- The best safety and privacy practice is to keep the minimum amount of information necessary to address her needs, and to delete information once it is no longer accurate or needed.

WHAT MIGHT AGENCY RECORD KEEPING ABOUT AN ELECTRONIC MESSAGE LOOK LIKE?

Sample VAW Program Practice:

- Keep electronic messages for the minimal time necessary to address needs.
- To better protect the confidentiality and privacy of senders, have a regular schedule for reviewing and purging electronic messages from your system.
- Record the minimal information necessary to provide support and to document what the agency provided. Redact or delete what you don't need.

There are many ways to do accurate documentation without connecting it to personally identifying information. Designing privacy into your record keeping can increase safety for women. Agency record keeping might involve filling out a checklist documenting:

- Date/time of contact:
- Time spent:
- Contact method: social media.
- Issues: for example, technology-enabled abuse, harassment by ex boyfriend.
- Discussed:
  - Technology safety and privacy planning.
  - Spyware and device monitoring.
  - Simple ways to log and document technology-enabled abuse.
  - Local contacts for police and trauma-informed care

REASONS NOT TO KEEP THE WHOLE EMAIL, INSTANT MESSAGING THREAD

Personal and private information about survivors is highly sensitive information.

- What private and personal information does her email include that is not needed for the agency to provide appropriate support?
- Does it include any personally identifying information about other people (for example, people she knows but who have not received services from this agency)?
- Does it include any personal information about unrelated past abuse that she or someone else experienced (for example, childhood sexual abuse, rape as a teenager)?
- Adding it to the agency file about her may not be what she wants.
- When she wrote the email, who did she think would read it? If she considers her email private correspondence to an individual staff member who has been very supportive to her, how might it violate her privacy rights to place the full email into a file the agency is keeping?
- The more sensitive information your agency keeps, the higher the risks and potential agency liability if your office or your computer networks are hacked.

MINIMAL INFORMATION PROTECTS SAFETY AND PRIVACY

For decades, when VAW program staff communicate with a survivor in person or over the phone, we listen carefully and jot brief notes to help us better support her needs.

- Technology has long been available to do it, but do not transcribe or record all of our confidential conversations with the women and youth we support.
- The best practice for agencies that use TTY machines to communicate with women who are deaf, is to document the caller's needs and what the agency does. We do not recommend printing a transcript of the entire conversation to place in her agency record. If a temporary printout is made, it should be shredded once no longer needed.
- For agencies that install security cameras to watch their women's shelter or transition houses, the best privacy practice is to routinely delete/overwrite those video tapes. The relevant portion of a tape is only retained if it documented criminal acts, such as a stalker trespassing, snooping in windows, violating a protection order or harming a woman. The rest of the tape that might show women coming and going, would be deleted to protect their confidentiality, privacy and safety.
- Similarly, for agencies that receive emails, text messages, video calls (for example, Facetime), or other communications via an agency's social media or other account, the best default privacy and safety practice is to document relevant information and then delete/shred/redact what isn't relevant.

3.8 Collecting Evidence and Reporting Violations

SUPPORTING SURVIVORS WHO WANT TO REPORT

- How will you support survivors so they can keep their own documentation of technology-enabled abuse?
  - Survivors can log what is happening. They can write down date and time, number and length of harassing messages/calls, and what she felt upon receiving the technology-enabled abuse.
  - Survivors can use technology to help them save evidence. For example, they can take screenshots of threats sent via text message, and save web versions of social media postings as PDF files.
- How will you support survivors in making their own reports to social media sites or when contacting the police?

WHEN WILL YOUR AGENCY COLLECT EVIDENCE OR REPORT VIOLATIONS?

- What types of problematic or abusive postings will your agency document?
  - For example, what if perpetrators or members of the public use your agency's social media account to threaten agency staff, or a woman or child who is accessing your program?
- How will your agency document incidents?
  - For example, will you take screenshots of messages and user IDs, print Web pages as PDF files, log what happened, and how employees/participants said it impacted them?
  - How deep will your social media research and documentation of abusive or potentially criminal incidents go?
  - How will you involve and meet the needs of staff and participants who are impacted by the incident your agency wants to document?
  - How will you best protect employee/participant confidentiality, privacy and safety rights during the documentation process?
  - Since some police reports can become public records, can you redact information that is swept up in the documentation but is not necessary to include, or that employees/participants want kept confidential/private?
- When will your agency file a report with the social media site?
- When will your agency have police investigate, collect evidence and file a report?
- How will your agency address media involvement or interest in any of the above situations?

3.9 Copyright and Terms of Use

Make sure your agency is legally allowed to use the content you post or share via the agency's website or social media accounts. Content creators and owners can restrict or grant the right to use or adapt their work. They can restrict use to specific purposes (for example, non-commercial) and require you post specific wording to credit creators and performers.

Do you want to let others use your resources but still protect your original content?

- Creative Commons Tools (http://creativecommons.org/choose) provides one internationally recognized easy way to grant "some rights reserved" licenses. You can use Creative Commons Tools to designate permissions for the works you own and share via social media.

How can you use other people's content and work?

- Get permission. Before contacting them, check if the file includes distribution permissions, or, displays Creative Commons symbols to indicate permitted use.
- The Fair Dealing[35] exception to Canadian copyright law permits certain uses of content—for research, private study, education, satire, criticism, review or reporting news. Consider how this applies to content you and others share on social media.

SOCIAL MEDIA TERMS OF USE

Most social media sites have Terms of Use that make site users solely responsible for the "user content" they post.

- Organizations are often made responsible for user content posted on their behalf by designated users of their social media account.[36]
- Ethically, VAW programs should consider it their responsibility to regularly monitor the user content posted on their social media page by staff and others.

Many social media sites have Terms of Use that say:

- "You own all of the content and information you post" on this site.[37]
- By posting content via your social media user account, you give the social media company the right to use your intellectual property (IP) in many ways for free.
- If you delete your social media account and content, but other users have already shared your content, the social media site can still use your content.[38]

[35] Wikipedia. (2013 August) Fair Dealing in Canadian Copyright Law. Available at: http://en.wikipedia.org/wiki/Fair_dealing_in_Canadian_copyright_law

[36] For example, Pinterest Terms of Service state that: *"If you open an account on behalf of a company, organization, or other entity, then (a) 'you' includes you and that entity, and (b) you represent and warrant that you are authorized to grant all permissions and licenses provided in these Terms and bind the entity to these Terms, and that you agree to these Terms on the entity's behalf."* Retrieved at: http://about.pinterest.com/terms/

SUPPORTING SURVIVORS OF TECHNOLOGY-ENABLED ABUSE

Being familiar with copyright issues and social media terms of use can be helpful if you do personal privacy and safety planning with women, youth, and survivors who have had photos or other content shared via social media without their permission.[39]

- CIPPIC has a FAQ on Canadian Copyright and Privacy in Photography at: http://www.cippic.ca/en/FAQ/Photography_Law

[37] For example, Facebook's Statement of Rights and Responsibilities (2012 December) says: "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings." Retrieved at: http://www.facebook.com/legal/terms

[38] For example, Facebook's Statement of Rights and Responsibilities (2012 December) says: "For content that is covered by intellectual property rights, like photos and videos (IP content)….you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it."

[39] CIPPIC has information on Canadian Copyright at: http://www.cippic.ca/en/copyright and on Copyright and Privacy in Photography at: http://www.cippic.ca/en/FAQ/Photography_Law.

4. Create Your Social Media Presence

Here are some practice considerations when creating a social media presence:

4.1 Will You Have a Private or Public Social Media Presence?

- Consider who your target audience is. Discuss the benefits of private Wikis, blogs, Twitter accounts and closed social media groups. Not all social media is public.
- Assess if your goal and objectives are better addressed by creating and engaging participants in a social media space with restricted access.
- In either space, make it clear that it's ok for people to disagree, share different opinions and to debate issues and solutions. In fact, the freedom to voice your different experiences and perspectives is a healthy part of democratic society. Demonstrate how your agency values the different opinions of a diversity of women, youth and survivors.

4.2 How Will You Provide Clear and Transparent Notice?

- How will you let people know who to contact and where to go in a crisis?
- How will you alert visitors that some perpetrators use spyware[40] to secretly monitor a survivor's device or activities (for example, computer, mobile phone, location, conversations, Web browsing, text messages)?
- Where will you suggest that survivors of technology-enabled abuse consider using a safer computer or mobile phone (for example, a computer at a public library or a donated phone from a women's shelter) if they think someone abusive is monitoring them?
- How will you remind visitors how public or private your social media space is?

- How will visitors learn about your purpose, available services, hours, contact information and general location (Canadian town/county, province/territory)?
- Will people be able to contact your agency via your social media account?
  - If yes, how long it will take your agency to respond to messages sent via your social media account? (for example, 3–5 working days) Are there ways to let people know this before they contact you?
  - What will your safety protocol be for responding to women who send messages to your social media account requesting help, or describing experiences of technology-enabled or other abuse?

[40] NNEDV. (2008) Who's Spying on Your Computer? Spyware, Surveillance and Safety for Survivors. Available at: www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_English.pdf and Qui Vous Espionne Lorsque Vous Utilisez Votre Ordinateur ? at: www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_French.pdf

4.3 How Will You Respond to Things Visitors Post On Your Social Media Page?

Your vision, values, goals and objectives should guide considerations about which posts you respond to, review, document, remove and/or report.

- What content will you post to your agency's social media channel/wall/pages?
- Will you let visitors respond to your posts on your channel/wall?
- Will you let visitors post separate things on your channel/wall?
- What questions can staff answer on an agency's wall/channel/feed?
- How will you filter, monitor or moderate posts by visitors to agency pages?
- What criteria will you use for evaluating problematic posts?
- If you remove a post, will you post a public message explaining the removal?
- Under what circumstances will you send a message to the author of a post your agency removes?
- When will you block a user from posting to your agency's wall/channel, or from following your feed?

Create general explanations and responses that can be adapted by staff when they need to respond to problematic posts and delicate safety situations.

- Remember, once a post is made, it is never truly gone. Anyone might have documented or shared the post before it was deleted.

- How will your agency address requests or posts from survivors?
- How might you discreetly raise awareness about the potential risks of posting personal information on a public social media page?
- How will you provide crisis and helpline information so they are aware of other ways to quickly seek support?

VAW agency policies may vary based on staff capacity and the purpose of their social media presence. Some policies:

- Tell staff not to engage in any online public discussions about women, youth and survivors who are current or former VAW program participants/ residents.
- Provide staff with adaptable generic responses they can use on a case-by-case basis if public conversations about private information arise on the agency's social media channel/page/feed. These adaptable responses aim to raise awareness of privacy risks and encourage posters to use private methods to discuss personal and private information.

- What types of problematic or abusive postings will your agency document?
  - For example, what if perpetrators or members of the public use your agency's social media account to threaten agency staff, or a woman or child who is accessing your program?
- How will your agency document incidents?
  - For example, will you take screenshots of messages and user IDs, print Web

pages as PDF files, log what happened and how employees/participants said it impacted them?

  - How deep will your social media research and documentation of abusive or potentially criminal incidents go?
  - How will you involve and meet the needs of staff and participants who are impacted by the incident your agency wants to document?
  - How will you best protect employee/participant confidentiality, privacy and safety rights during the documentation process?
  - Since some police reports can become public records, can you redact information that is swept up in the documentation but is not necessary to include, or that employees / participants want kept confidential/private?
- When will your agency file a report with the social media site?
- When will your agency have police investigate, collect evidence and file a report?
- How will your agency address media involvement or interest in any of the above situations?

4.4 How Far Reaching or Interconnected is Your Digital Space?

- What are you sharing? How is it being interpreted and discussed?
- How you are going to be part of that ongoing conversation?

5. SOCIAL MEDIA POSTS: DATA PRIVACY AND PERSONALLY IDENTIFIABLE INFORMATION

Social media posts are regularly shared further than the author of the original post realizes. Even if privacy settings restrict who initially sees the post, the post can still end up being shared with more people. Most social media sites strongly promote a culture of "sharing" information. Things staff and survivors share can be reposted or posted on multiple social media sites (for example, an Instagram[41] photo can be posted simultaneously to Twitter, Facebook, Tumblr, Foursquare, Flickr and more). Posts to an agency's social media page/channel are often available to the public.

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.
- Discuss the legal, confidentiality and safety risks that could arise if a VAW program participant/resident were to post details about recent experiences of sexual or domestic violence on your agency's public social media space/channel/page.
- Decide whether, on a case-by-case basis, you will privately contact people who post details about abuse on your agency's public channel/feed.
    - As an agency, discuss various scenarios and identify potential risks and benefits.
    - Review your agency practices about the safest ways to respond to voice mail messages, emails, instant messaging and text messaging.
- If your agency does contact someone privately via social media, remember:
    - Posting on your agency's social media space might be a difficult and brave act. Affirm the right of survivors to speak out about their experiences.
    - Posters may use some privacy settings but still not be aware of several safety, privacy and legal risks of public social media posts.
    - Let posters know what your agency can provide, and other ways to contact you. Offer more resources.
    - Offer to strategize about the benefits and risks of public posts.
    - Don't assume that the visible social media identity is accurate. Survivors sometimes use pseudonyms, and perpetrators sometimes impersonate survivors and others.

[41] Instagram. (2013) How do I share from Instagram to other social networks? Available at: http://help.instagram.com/365696916849749

- 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.
- Make sure to address confidentiality, security and record keeping and other issues covered in section 2: Legal and Ethical Issues of this guide.

6. SOCIAL MEDIA AND ACCESSIBILITY

It is important to support the rights of people with varying abilities, to use the social media/network tools they choose in the most accessible way.[42]

Social media's constant evolution impacts how accessible your agency's social networking spaces and activities will be to different people with varying abilities. When VAW programs evaluate what social media tool to use, they should review and consider:

> "While social media networks still present access barriers, there are steps organizations and individuals can take to reduce them."[18]
>
> ~Media Access Australia

- Which social media applications are currently accessible, to what extent, and to whom?
- Do they have a reliable history of designing accessibility into each upgrade?
- Does the level of accessibility change depending on the device or application being used? Do common and popular assistive technologies work and integrate easily with the social media application?
- Which social media applications are not very accessible?
- How can people with disabilities best use the popular social media tools that you are reviewing and considering?
- Are there different ways you can use your current social media tools to increase accessibility or decrease accessibility?

[42] Media Access Australia. (2011) Sociability: Social Media for People with a Disability. Available at: http://www.mediaaccess.org.au/online-media/social-media

7. STAYING CURRENT

When assessing your program's capacity to engage in social media, it is also important to take into account that social media/network applications are constantly evolving and being upgraded. Users are often not notified. VAW programs must have the capacity to stay current with these changes. Sometimes, when privacy and security settings are upgraded, they are automatically reset to default settings that are less private and secure. VAW programs using social media must have the capacity to stay aware and check their settings often. Not doing so can have unintended consequences for women, youth and children accessing a VAW program's social network or media application.

8. SUPPORTING WOMEN, YOUTH AND CHILDREN

Women, youth and children will often join your social media/network pages to stay connected to your agency. When developing your social media communication plan, it is helpful to keep in mind that survivors are part of your audience. This will help you address privacy, confidentiality and safety risks.

When supporting survivors, it is important to develop practices about safety plans that address your program's social media presence. Let them know they are welcome to participate; however, posting on your page can have implications to their safety as social media pages are often not private. Also discuss that if survivors request help through your social media page, that someone in your agency may not be able to respond right away. Providing alternative contact information like crisis lines can be helpful when planning for one's safety.

On your social media pages, educate and alert visitors of the potential safety and privacy risks that can arise for those experiencing technology-enabled abuse. Discuss risks like:

- Adding your agency as a "friend", cause and/or group.
- Posting to your social media page/space/feed.
- Rapists and abusers who stalk and impersonate survivors on social media sites.
- Defense attorneys who try to get access to information about rape survivors from social media sites.

8.1 Safety Strategies: Giving Up Social Networks is Not the Only Option

Social media and networks may be a helpful support system for survivors and their families. If a woman changes college campuses after a sexual assault, or relocates her family to flee an abusive ex-boyfriend, social media might be used to decrease isolation and keep her connected to people she trusts. It is empowering to develop practices where survivors can be educated on safer ways to use technology, rather than giving it up. When safety planning, here are some questions to consider for women and youth fleeing technology-enabled abuse:

- Who might respect your heightened need for online privacy and safety?
- Which "friends" (family, friends, acquaintances)?
- What changes might you and those "friends" need to make to social networking settings?
- What kinds of conversations might you want to have with VAW programs and select "friends" to help you decide?
- What are the privacy/content policies of the site you are using or want to use?
- When might reporting violations to the site and police be a helpful safety strategy?

9. PERPETRATORS' MISUSE OF SOCIAL NETWORKS AND MEDIA

It is helpful to do safety planning with survivors about their own social media use. Perpetrators of family and dating violence, sexual violence and harassment, stalking and bullying now regularly misuse social media and networks to stalk and harass. They locate, threaten, coerce, target and terrorize women, youth and children. Some of the tactics of technology-enabled abuse that perpetrators employ in social media:

- Create fake accounts of the woman or youth, or of her friends or family members, to impersonate and gain more information about her.
- Monitor the survivor's (and her children's) social media pages to find the location of their schools, and other activities they are participating in. Stalkers also establish patterns by monitoring the location and timing of posts.
- Post nude or semi-nude photos and videos of women, youth and survivors.
- Harass, coerce and/or threaten a woman or youth through social media posts or private messages.
- Post harassing or inappropriate messages on the survivor's friend's pages as well as agency pages.
- Monitor her page and coerce her into updating certain things.
- "Friend" the survivor's friends and family through social networks.
- Gather personal information through search engines and public profiles.
- Hack her passwords and take over her social media and/or social network accounts.
- Create false social media identities and harass her online.

Anti-violence workers can safety plan with survivors about technology-enabled abuse through social media. This includes discussing:

- Changing account settings to increase privacy, security, notifications and blocking.
- Temporarily decreasing, changing or stopping posts.
- Safer ways to post comments or news.
- Safer ways to post pictures, and how to remove location information from pictures.
- Thinking carefully about what gets posted by the survivor, and who might eventually see or share it with the abusive person.
- Changing the "tag" settings so that tagged posts and pictures must be reviewed.
- How to report or flag inappropriate pictures, posts and content.
- Documenting threatening, harassing messages, such as how to capture a picture of their Smartphone or computer screen, printing a webpage as a PDF file, and other options.
- How to opt in and opt out of various automatic location services.
- Ways to remove location information and geotags from photos, tweets and posts.
- Refraining from revealing location through "Check In" to places.
- Creating a new profile with a private smaller set of “friends” who will commit to protect your privacy.
- How most sites have a process for users to report if their account has been compromised.
    - Hacking or misusing a survivor’s social media account may be a violation of an order, or of part of a stalking or harassment charge.

10. MEASURING SUCCESS WITHOUT COMPROMISING SAFETY, PRIVACY AND AUTONOMY

> "Measure what you value, and others will value what you measure."
>
> ~John Bare, The Arthur M. Blank Family Foundation[29]

VAW programs face distinct challenges in measuring if we are being effective in our social media activities. Because of the high risks faced by the women, youth and survivors we work with, our anti-violence agencies and VAW programs need to even carefully critique the technology we might use to automatically measure our progress. Social media engagement takes staff time and agency resources. It takes even more time if you commit to measure your impact, learn from your mistakes, and ensure your social media activities remain consistent with your values, vision, goals and objectives. Here are a few things to keep in mind.

10.1 Website and Social Media Analytics

When you have a social media or website presence, there are many automated free and low-cost tools you might use to measure how people engage with your online content. There are analytical tools that will automatically count which Web pages visitors view and what files they download,[43] which of your Facebook posts get the most likes and comments, or which tweets get the most retweets.

[43] Google Analytics is the most widely used service for website analytics and offers Mobile App analytics, Tag Management and more. Available at: http://www.google.com/analytics and http://en.wikipedia.org/wiki/Google_analytics/ .

TICK TO YOUR VALUES. AVOID TOOLS OR ACTIONS THAT REPLICATE WOMEN'S EXPERIENCES OF TECHNOLOGY-ENABLED ABUSE AND ONLINE MONITORING.

- Perpetrators use spyware to stalk women online, on computers and via mobile devices. It is easy for stalkers to use spyware to stalk their spouse, ex, girlfriend, children or a person they plan to rape. Spyware secretly installed on mobile devices or desktop computers can track location, keystrokes, take screenshots, record conversations, forwarded email and text messages, and more.[44]

Some companies are marketing in-page/visual analytics as "customer experience analytics." They promise to monitor your visitors' mouse moves, clicks and page scrolls, take screenshots as your visitor moves around your pages, and attempt to associate as many unique or personal identifiers as possible with the individual website visitor. This type of online analytics raises significant privacy concerns.

10.2 Outcome Measurements that Value Safety, Privacy and Anonymity

- Many online analytic tools measure increases in quantity or outputs. How will you communicate to funders and supporters when quantity is a useful indicator of social media success, and when and why it is not?
- Are there ways you can express, even anecdotally, how your agency's upfront notice and transparency is enhancing safety and privacy for women, youth and other survivors? For example, these are successful outcomes:
  - If a woman or youth reads your online safety alerts and decides it is safer or more private for her to "not actively follow or like" your page.
  - If a survivor decides to quickly leave your social media channel or website, because your online safety information immediately alerted her that some abusive spouses use spyware to monitor computer or mobile devices.

[44] NNEDV. (2008) Who's Spying on Your Computer? Spyware, Surveillance and Safety for Survivors. Available at: www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_English.pdf and Qui Vous Espionne Lorsque Vous Utilisez Votre Ordinateur ? at: www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_French.pdf

EDUCATING ABOUT PRIVACY TOOLS

If VAW programs provide upfront notice and information about ways to enhance safety and privacy when using social media, then more women, youth and survivors will use online safety and privacy tools. Many of these privacy tools block the effectiveness of popular Web analytic tools.[45] If we do our jobs well, our statistics may be artificially lowered and the count of visitors from non-Canadian locations may seem artificially high. But, women will be using more tools and strategies that help protect their privacy online.

JUST BECAUSE IT CAN BE FOUND, COLLECTED OR DOCUMENTED DOESN'T MEAN YOU SHOULD

Social media has amazing potential to decrease isolation and transform lives, but it also compiles a lot of personal data about women and youth that may not be accurate, or may not be information they choose to share with your agency or VAW program. Listen to what is important to different women, youth and survivors of violence. Think about how to tell those stories. Then, "measure what you value, and others will value what you measure".[46] For example, measure:

- Ways that our online actions actively promote (and do not accidentally undermine) the safety, privacy and wellbeing of women, youth and children.
- How to engage with social media in ways that enhances education, options, safety and supports for survivors currently experiencing technology-enabled domestic and family violence, sexual violence and harassment, stalking, dating abuse and other online violence against women.

Measure your impact, learn from your mistakes, and ensure your social media activities remain true to your values, vision, goals and objectives.

[45] Several privacy tools affect the accuracy of automated Web analytics tools. For example, some privacy tools delete or block the Web browser cookies or beacons that advertisers and Web analytics tools use; privacy tools like online anonymizers, mask the user's actual location and provide a different geographic location. Wikipedia. (2013 September) Google Analytics. Retrieved at: http://en.wikipedia.org/wiki/Google_analytics/

[46] Bare, John. (2005) Evaluation and the Sacred Bundle. *The Evaluation Exchange, XI* (2), Retrieved at: http://www.hfrp.org/evaluation/the-evaluation-exchange/issue-archive/evaluation-methodology/evaluation-and-the-sacred-bundle

11. SOCIAL MEDIA RESOURCES FOR NONPROFIT VAW PROGRAMS

11.1 For Nonprofits Exploring Social Media

Idealware. Helping Nonprofits Make Smart Software Decisions. (USA)
http://idealware.org

- Exploring Cutting Edge Social Media. (2013) http://www.idealware.org/reports/cutting-edge-social-media
- The Nonprofit Social Media Decision Guide. (2011) http://www.idealware.org/reports/nonprofit-social-media-decision-guide
- Nonprofit Social Media Policy Workbook. (2012) http://www.idealware.org/reports/nonprofit-social-media-policy-workbook
- Social Media Policy Template. (2012, use with social media policy workbook) http://www.idealware.org/smpolicy
- Social Media Resource Library. (2010, ongoing additions) http://www.idealware.org/reports/social-media-resource-library
- What Every Nonprofit Should Know About Mobile: Lessons from Global Development Nonprofits. (2012) http://www.idealware.org/reports/mobile-global-development

Canadian Internet Policy and Public Interest Clinic/la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko. (CIPPIC) http://cippic.ca

- Social Networking (2008, 2012) http://cippic.ca/en/FAQ/social_networking

Electronic Privacy Information Center. (USA).

- Social Networking Privacy (news updates) http://epic.org/privacy/socialnet

Facebook.

- Building your presence with Facebook Pages: A guide for causes and nonprofits. (2013 March) https://fb-public.app.box.com/s/8dxyv66biabfnesvr3jj

Nonprofit Tech for Good. A Social and Mobile Media Blog for Nonprofits. (USA).
http://www.nptechforgood.com

Google for Nonprofits Blog. http://googlefornonprofits.blogspot.com

- Google+ Best Practices for Nonprofits. (2013 August) Available at: http://services.google.com/fh/files/misc/finalgoogleplus-fornonprofits.pdf

Social Media Governance. Empowerment with Accountability. (USA).
Online Databases of Government and Non-Profit Social Media Policies.
http://socialmediagovernance.com/policies.php?f=5

Tech Soup Canada (www.techsoupcanada.ca).

- Community and Social Media: www.techsoupcanada.ca/taxonomy/term/282

11.2 Accessibility of Social Media

Adaptech Research Network. (Canada). Free and Inexpensive Adaptive Technology Database. http://adaptech.org/en/downloads	Réseau de Recherche Adaptech. (Canada). Base de données de technologies gratuites ou peu coûteuses. http://adaptech.org/fr/telechargement
Media Access Australia. (Australia). • Sociability: Social Media for People with a Disability. (2011) http://www.mediaaccess.org.au/online-media/social-media	
WebAIM. (USA) • Captioning Resource List (Tutorials, Tools, Services). http://webaim.org/resources/captioning	

11.3 Education and Awareness Campaigns

Draw the Line. www.draw-the-line.ca Sexual violence prevention campaign	Traçons les limites. www.tracons-les-limites.ca une campagne de prévention de la violence à caractère sexuel
Media Smarts: Canada's Centre for Digital and Media Literacy. http://mediasmarts.ca	HabiloMédias: le centre Canadien d'éducation aux medias et de littératie numérique. http://habilomedias.ca
Need Help Now.ca. You(th) are not alone. http://needhelpnow.ca	Aidez Moi SVP.ca. Les jeunes ne sont jamais seuls. http://aidezmoisvp.ca
A Thin Line. Draw your line btwn digital use/digital abuse. http://www.athinline.org MTV's sexting, textual harassment, cyberbullying and digital dating abuse campaign.	
That's Not Cool. Where do you draw your digital line? http://www.thatsnotcool.com Public education campaign to raise awareness about and prevent teen dating abuse.	

11.4 Mobile Apps and Online Games

Metropolitan Action Committee on Violence Against Women and Children. (Metrac). http://metrac.org • "Not Your Baby." iPhone app generates peer responses to sexual harassment situations. http://itunes.apple.com/us/app/not-your-baby/id545191859?mt=8. • "What It Is. A digital game Challenging Sexual Violence." Online game for ages 12–15. http://challengesexualviolence.ca

• "RePlay: Finding Zoe/ReJouer: Où est Zoé?" an online game about healthy relationships for ages 8–14. http://metrac.org/replay/index.html	
Office of the Privacy Commissioner of Canada (OPC). • myPRIVACYapp. A Privacy Mobile Application with 10 steps to help better protect your privacy on mobile devices. www.priv.gc.ca/resource/tool-outil/app/index_e.asp	Commissariat à la protection de la vie privée du Canada (CPVP). • applimaVIEPRIVÉE. Une application mobile pour la protection de la vie privée propose 10 mesures qui vous aideront à vous prémunir contre les atteintes à votre vie privée sur votre appareil. www.priv.gc.ca/resource/tool-outil/app/index_f.asp
Securiguard. http:/securiguard.com and Ending Violence Association of BC. http://endingviolence.org • "SOS Response." Smartphone app. In an emergency, press button and 30 photos are immediately taken and sent with your location to a 24/7 monitored security service that coordinates with local emergency authorities. http://sos-response.com/eva	
YWCA Canada. http://ywcacanada.ca • "Safety Siren." Smartphone app. Sends emergency alerts to contacts you choose and sounds Siren alarm when pressed. App includes a national directory of resources. http://ywcacanada.ca/en/pages/mall/apps.	

11.5 Safety and Privacy for Survivors and Agencies

Canadian Clearinghouse on Cyberstalking http://www.cyberstalking.ca/en	Centre canadien d'information sur le cyber-harcèlement http://www.cyberstalking.ca/fr
National Network to End Domestic Violence, Safety Net Project. (USA) Technology Safety Resources. http://nnedv.org/resources/safetynetdocs • Cell Phone: Location Tracking and Sharing. (2011) www.nnedv.org/resources/safetynetdocs/1022-cell-phone-location-track.html • Cell Phone and Location Safety Strategies. (2013) www.nnedv.org/resources/safetynetdocs/3842-cellphone-safety-planning.html • Online Privacy and Safety Tips. (2010) www.nnedv.org/resources/safetynetdocs/online-privacy-a-safety-tips.html • Privacy Considerations When Posting Content Online. (2010) www.nnedv.org/resources/safetynetdocs/419-privacy-considerations-when-posting-content-online.html • Privacy and Safety on Facebook: A Guide for Survivors of Abuse. (2013) www.nnedv.org/resources/safetynetdocs/3868-facebook-privacy-safety.html • Safety in a Mobile World: A Look at "Apps." (2012) • Sexting. (2011) www.nnedv.org/docs/SafetyNet/OVW/NNEDV_Sexting_2011.pdf • Social Networking and Privacy Tips for Domestic and Sexual Violence Programs. (2012) www.nnedv.org/resources/safetynetdocs/social-networking-a-privacy.html	

<table>
<tr><td colspan="2">• Tech Safety Quick Tips. (2011) http://tools.nnedv.org/tipsheets-charts/charts/110-technology-safety-quick-tips</td></tr>
<tr><td>• Tech Savvy Teens. Choosing Who Gets To See Your Info. (2009) www.nnedv.org/docs/SafetyNet/NNEDV_TechSavvyTeens_English.pdf</td><td>• In Spanish—Adolescentes Tecnisabios: Escoge Quién Pueda Ver Tu Información. (2009) www.nnedv.org/docs/SafetyNet/NNEDV_TechSavvyTeens_Spanish.pdf</td></tr>
<tr><td>• Who's Spying on Your Computer? Spyware, Surveillance and Safety for Survivors. (2008) www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_English.pdf</td><td>• Qui Vous Espionne Lorsque Vous Utilisez Votre Ordinateur ? (2008) www.nnedv.org/docs/SafetyNet/NNEDV_SpyWareAndSafety_French.pdf</td></tr>
<tr><td>Office of the Privacy Commissioner of Canada (OPC)
• Social Networking and Privacy. (2007) www.priv.gc.ca/resource/fs-fi/02_05_d_35_sn_e.asp</td><td>Commissariat à la protection de la vie privée du Canada (CPVP)
• Établissement de sites de réseautage personnel et protection de la vie privée. (2007) www.priv.gc.ca/resource/fs-fi/02_05_d_35_sn_f.asp</td></tr>
<tr><td colspan="2">Pennsylvania Coalition Against Rape; Pennsylvania Coalition Against Domestic Violence. (USA)
• Tech Top 10 Guidelines. Social Media Use by Programs and Staff. (2011) http://www.ncdsv.org/images/PCAR-PCADV_TechTop10TipsSocialMediaUseByProgramsStaff_2011.pdf
• Assisting Survivors with Personal Privacy Management: Digital Technology and Safety Information Booklet. (2012—for use by advocates) http://ncfy.acf.hhs.gov/sites/default/files/docs/21447-Assisting_Survivors_With.pdf
• Safety Tips for Using Computers and Cell Phones. (2012) http://pubs.pcadv.net/clr/TechTips_for_Survivors.pdf</td></tr>
<tr><td colspan="2">Privacy Rights Clearinghouse. (USA)
• Social Networking Privacy: How to be Safe, Secure and Social. (2013) www.privacyrights.org/social-networking-privacy
• Privacy In the Age of the Smartphone. (2013) www.privacyrights.org/fs/fs2b-cellprivacy.htm</td></tr>
<tr><td>Sex Information and Education Council of Canada (SIECCAN)
• Sexting: Considerations for Canadian Youth. (2011) http://sexualityandu.ca/uploads/files/CTRsextingEnglishApril2011.pdf</td><td>Le Conseil d'information et d'éducation sexuelles du Canada
• Le sextage : Aspects à envisager pour les jeunes Canadiens. (2011) http://sexualityandu.ca/uploads/files/CTRsextingFrenchApril2011.pdf</td></tr>
<tr><td colspan="2">VAWnet: National Online Resource Center on Violence Against Women. (USA)
• Special Collection: Safety and Privacy in a Digital World. (2013)</td></tr>
</table>

http://www.vawnet.org/special-collections/TechSafety.php

11.6 Safety Net Canada via Social Media

Subscribe to: http://youtube.ca/SafetyNetCanada
For playlists of videos that include safety, privacy, accessibility and social media tips.

Follow our Tweets! http://twitter.com/SafetyNetCanada
For recent news on safety, privacy, accessibility, social media and technology-enabled abuse.

11.7 Safety Net Canada National Reports

Executive summaries are written in English and French.
Les sommaire de gestion sont écrits en anglais et en français.

- Assessing Technology in the Context of Violence Against Women and Children. Examining Benefits and Risks. (2013)
- Canadian Legal Remedies for Technology-Enabled Violence Against Women. (2013)
- Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy and Confidentiality of Women, Youth and Children. (2013)

11.8 Safety Net Canada National Surveys

- Safety Net Canada Summary Report: Survey of Canadian Anti-violence Workers on Technology Abuse. (2012)
- Safety Net Canada Summary Report: Organizational Technology Practices Survey for Canadian Violence Against Women Programs. (2013)

- Infograph: Technology Misuse and Violence Against Women Survey. (2013)
- Infographique: Résultats d'un sondage sur les abus technologiques à des ns de violence envers les femmes. (2013)