Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children.

Safety Net Canada 2013

SAFETY NET

ACKNOWLEDGEMENTS

We are indebted to many people for providing insights and other contributions towards this project. While the opinions expressed in these reports are ours alone, they are informed by years of collaborating with and learning from survivors, colleagues and communities.

We remain guided by the women, youth, and children experiencing violence at the hands of perpetrators. They often face high risks to their lives and wellbeing. We deeply appreciate all we continue to learn from these strong, brave, and creative individuals. Only by listening to the experiences and opinions of these women and youth, can Canada accurately identify and implement practices that best protect their safety, privacy, safety autonomy, equal rights and access to justice.

Thank you to the many anti-violence workers throughout Canada who contributed by sharing their experiences and knowledge for this report and for participating in our two national surveys of anti-violence workers on *Technology Abuse* and on *Organizational Technology Practices*. These individuals work in non-profit women's shelters, transition and interval houses, rape crisis centres, victim services agencies, counseling services, children exposed to violence programs, crisis lines, K-12 classrooms, college campuses, courts, income assistance offices, police stations, hospitals, mobile clinic vans, and many other places where a survivor of violence might request help. During this recession, many anti-violence programs face staff cuts, limited agency resources, and low salaries. These workers often volunteer time as crises arise and still took the time to fill out our surveys.

We gratefully acknowledge the Office of the Privacy Commissioner of Canada for providing funding for our research and this report and for their leadership. Privacy is priority concern for many women and youth, especially since it impacts their ability to maintain autonomy and access safety.

Thank you to CIPPIC legal interns Ken Dunham and Paul Holden for helping to review literature and compile findings and to CIPPIC Director David Fewer for supervising their work. Thank you to the U.S. National Network to End Domestic Violence's Safety Net Project for their ongoing leadership and support, and for providing a framework for our national technology surveys. A special thank you to Rhiannon Wong for her stewardship of this year-long project.

Thank you to Cynthia Fraser, founder of Safety Net Canada, who has been and continues to be an invaluable resource. We are grateful for having the opportunity to learn from you.

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

Research, Writing, Editing:	*Cynthia Fraser*
	Rhiannon Wong
	NNEDV Safety Net Project
French Translation:	*Jose Beaudet*
Graphic Design:	*Hannah Lee*

FINANCIAL CONTRIBUTION

We thank the Office of the Privacy Commissioner of Canada for their financial contributions to this work and project.

Office of the Privacy Commissioner of Canada / Commissariat à la protection de la vie privée du Canada

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 · NNEDV National Network to End Domestic Violence · Safety Net

Organizational Technology Practices For Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children.

EXECUTIVE SUMMARY

In Canada, there is a diverse range of anti-violence programs that focus on addressing, intervening, and preventing Violence Against Women and children (VAW Programs). They are crucial components in Canada's efforts to end violence against women, youth and children. VAW programs support women who are fleeing and/or living with the effects of gender-based violence including domestic/family violence, sexual assault, dating violence, stalking, bullying and criminal harassment. The structure and scope of these VAW programs not only vary within each province and territory, but also by rural, urban, or suburban geographies, and by the needs of the specific cultural communities living within a region.

The work that Canadian anti-violence / VAW programs undertake is extensive. They provide many confidential services that range from, but are in no way limited to: crisis and longer term support and counseling; 24 hour helplines; safety and privacy planning; risk assessment; accompanying women to visit or apply for another agency's services; legal and system advocacy; skills building such as employment and financial planning; emergency and transitional housing; drop in support centers or groups; health care; community outreach; culturally specific support; victim services; facilitated support groups; facilitated group classes; violence prevention and education programs; childcare and transportation; donated clothing and other goods; art and play therapy; and structured programs that support children who have experienced, witnessed, or been exposed to abuse (e.g. exposed to their father abusing their mother). In addition, Canadian VAW programs have many responsibilities in their communities and often support women, youth and children beyond their mandates.

Technology Use in VAW Programs

Increasingly, these services involve a technology component. Most agencies advertise phone services for the public which may include a 24/7 phone crisis line and TTY/TTD (Teletypewriter) service. Most agencies also receive both invited and unsolicited contacts via technology such as email, text messages, their website, Facebook, YouTube, or another social media site. In our 2013 "Organizational Technology Practices Survey for Violence Against women Programs" many VAW programs reported that they provide access to technology onsite for VAW program visitors, participants and residents: 73% provide landlines and 40% provide access to mobile

phones; 67% provide desktop computers and 27% provide access to laptops or mobile tablets; 35% provide video games, and 4% provide access to TTY/TTD machines.

23% of survey respondents provide Internet access to VAW program participants or visitors. 31% provided wireless Internet access for shelter/transitional housing residents and 17% noted that they provide program participants/residents/visitors with access to an Internet network that is separate from their staff/employee network. Providing computers and Internet access enables survivors the option to be supported in filling out online applications for housing, financial support or employment while staying safe in a shelter/house or visiting a VAW program. This is important, especially if the man abusing her is monitoring or spying on a computer she would otherwise be able to use. Providing access to technology and Internet can also reduce digital divides for women and youth who are homeless, have very low incomes, or where the abuser is doing both technology-enabled stalking and financial abuse. In the event that an abuser or stalker does show up at a rape crisis centre, shelter, or other anti-violence agency, 60% of surveyed VAW programs have security cameras installed outside their buildings.

Protecting Privacy and Confidentiality

95% of surveyed VAW programs store the information they collect as paper files in cabinets. About 45% store some information on an in-house server, 15% use a 3rd party hosted server, 19% use cloud computing or other online data storage, and 38% store this information on individual computers only (that are not attached to a network). A number of agencies noted that they store this information on thumb drives, data sticks, and external flash drives. Survey respondents did not specify which types of storage did or did not include information they collect about the women and youth they serve.

Practices vary widely for VAW programs that are using databases. 51% of surveyed VAW programs use databases to collect and store information about participants (aka women and youth who request and or receive services and support.) Some of these agencies keep identifying information on paper and use the database to submit aggregate non-identifying information to a government funder. Some collect basic information in a database for statistical purposes only. At least one VAW program said they collect statistical information that is not stored by them but is instead submitted to a government agency. Some agencies only document services provided, and others create an electronic participant/client record that holds personally identifiable information. A few programs said they collect statistical information that is not stored by them but is instead submitted to a government agency.

VAW programs also participate in community safety assessments as well as co-located and coordinated community responses with other sectors and services like justice, social and legal services, health, child protection, education and other nonprofit agencies. Examples of such collaborations include sexual assault response teams, disability response teams, domestic violence response teams, high-risk and fatality case review committees and community

coordination committees. Technology is being used in many ways during these collaborations, including to alert team members that they are needed, collect evidence, coordinate inter-agency services, and to share information. When anti-violence workers at VAW agencies do collaborations that involve co-location, this will sometimes mean that they work onsite at a police station or court house several days a week. How technology is used in these circumstances can enhance or undermine the confidentiality and privacy rights of woman seeking support. Clear boundaries in technology use and access to electronic information are critical to meeting mandates and protecting privacy and confidentiality when VAW programs collaborate or co-locate.

Technology Safety Planning

While VAW programs use technology to enhance their support services, anti-violence workers are also more frequently safety planning with women and youth who are living with the effects of traumatic, invasive and life threatening technology-enabled abuse.

This means, survivors and anti-violence agencies are now experiencing stalkers, abusers and rapists who hack computers and databases, threaten, impersonate, harass via email and social media, and steal confidential information via wireless networks and more. This is just a small sample of technology-enabled abuse, which makes it easier for perpetrators to carry out their often sole mission to track down and harm or kill his victim. This reality **makes it crucial for VAW programs to have organizational technology practices** that best protect the **safety, privacy, identity and confidentiality** of the women, youth, and children they serve.

It is important that VAW agencies include the use of technology in safety planning with women and discuss how perpetrators abuse, stalk, monitor, harass and impersonate via technology. Agency technology practices and policies must identify and address any security and privacy vulnerabilities that the perpetrator might exploit to try to access agency information or services. Precautions must also be taken to ensure that any technology agencies use is properly protected and secured to prevent perpetrators from acquiring additional information and doing further harm.

Organizational Technology Practices

Like the Canadian private sector, all VAW programs should be conducting privacy impact assessments and ongoing privacy risk management to ensure they use technology in ways that best protects identifiable, sensitive data of the women and youth they support. Program and agency policies and practices must take extraordinary measures to protect the confidentiality and identities of those they provide services to and must take every step they can to keep secure all personal, identifiable and confidential data collected, stored or used by staff and volunteers.

However, some VAW programs can face significant barriers in developing and implementing robust technology confidentiality, privacy, safety practices. Too many VAW programs face limited and unstable funding. Not all VAW programs have access to core funding for lights and heat, let alone technology security and maintenance. A minority of VAW programs have part time IT staff and even fewer have a full time IT staff person; more commonly, VAW programs have a small contract to keep an IT consultant on retainer as issues arise.

Responses to our 2013 "Organizational Technology Practices" survey echoed this reality. The number of staff in a VAW program ranged significantly from 1 to 225. Only 55% of survey respondents have a dedicated IT staff, company or consultant to attend to IT needs. When asked, the top barriers VAW programs face in developing such practices are: lack of funding (69%) and time (66%); lack of knowledge and training on technology or security steps (62%), or, on privacy and confidentiality laws and regulations (46%); how quickly technology changes and new technology appears (58%), and, the need for more examples, samples and adaptable templates (59%). Surveyed VAW programs requested more information be developed on a range of technology policies and practices including social media and networking, electronic communication, mobile phones and devices, technology in service provision, location tracking devices and services, data and databases, and technology safety, privacy and identity protection planning.

It is not surprising that these agencies want to develop and enhance their technology practices. Anti-violence agencies are organizing events online and offline to empower women and youth, support the voices of survivors, engage the community in preventing and ending violence, and honor the women and children who have died as a result of gender-based violence. Events and training announcements that were faxed a few years ago, are now distributed via email and posted on websites, Facebook and other social media pages. Event registrations are increasingly done via online forms or email. Some VAW programs are creating online or mobile phone campaigns and events. In such technology-enabled campaigns, participants might be asked to sign an online petition, make a financial donation, take and post photos, 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. Many VAW programs also provide community-based and age-appropriate school-based violence prevention and skills building programs. VAW programs have created intervention and prevention apps, videos, quizzes and games to empower women and girls. When engaging in any public outreach via technology, it is important to assess the potential impact on privacy, confidentiality, identity and safety. It is important to plan for technology changes that can create new risks years after the campaign is run.

Addressing privacy and security in a VAW programs' technology practices is important because how we use technology can increase or decrease safety risks for women and their loved ones. For example, policies and practices that involve "taking technology away" can be

disempowering to women and seem like a form of power and control. Asking women to turn off and turn in their technology does not tend to increase safety and can actually increase risks. As part of our commitment to supporting the autonomy, accessibility and self-determination of women and youth, Safety Net Canada does not recommend banning or taking away technology like mobile phones or computers. Instead we encourage all anti-violence agencies to build staff knowledge and skills so they can do ongoing safety planning with women about the risks and benefits of each technology. It is important to get commitments from participants and residents that they will not use technology to compromise the privacy, safety, identity confidentiality and security of other staff or participants. And it is important to be very concrete about what that means.

Regardless of our intentions, there are some technology practices that tend to have higher risks of interception. Without strong security measures (e.g. encryption) a decision to store women's information online or in electronic databases or to communicate about or with her via email or text messages can actually increase safety and privacy risks. The personal information we collect and store electronically, including a new address and phone number, can have unintended consequences and personal information can be easily intercepted and fall into the hands of her abuser or stalker. If VAW programs are committed to ending violence against women and girls, we must create policies and practices that enhance (not undermine) 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.

Technology can provide incredible benefits for VAW programs and the women and youth they support. It can also create significant vulnerabilities that increase risks to safety and privacy. Anti-violence agencies use technology in innovative ways to directly impact how communities discuss and engage in the movement to end violence against women and children. VAW programs must endeavor to not use technology in ways that increases risks for the women and children they support. That would go against mandates, missions and the reason that rape crisis centres and emergency shelters were created in the first place.

This report addresses important organizational practices related to the use of technology commonly used by anti-violence / VAW programs. It describes and recommends organizational technology practices that will enhance the safety and privacy of women, youth and children. It highlights issues to consider when developing or strengthening your anti-violence / VAW program's technology practices and includes some examples and scenarios that can help with evaluating technology practices. The goal of this resource is support VAW agencies in **enhancing their privacy and safety practices related to the use of technology.**

Pratiques organisationnelles de la technologie pour les programmes de prévention de la violence. Comment protéger la sécurité, la vie privée et la confidentialité des femmes, des jeunes et des enfants

SOMMAIRE DE GESTION

Au Canada, il existe plusieurs programmes de prévention de la violence faite aux femmes et aux enfants (VFF). Ce sont des programmes d'intervention et de prévention. L'existence de ces programmes est indispensable à l'effort du Canada pour mettre fin à la violence faite aux femmes, aux jeunes et aux enfants. Les programmes VFF aident les femmes, les jeunes et les enfants qui doivent fuir et/ou qui vivent avec les effets de la violence sexiste incluant la violence conjugale/familiale, l'agression sexuelle, la violence dans les fréquentations, la traque, l'intimidation et le harcèlement criminel. La structure et l'étendue de ces programmes VFF varient non seulement au sein de chaque province et territoire, mais aussi selon la géographie rurale, urbaine ou suburbaine et selon les besoins des communautés culturelles spécifiques qui vivent dans une région donnée.

Le travail entrepris par ces programmes canadiens de prévention de la violence/VFF est vaste. Ceux-ci offrent différents services confidentiels : aide et counseling dans des moments de crises et à long terme ; accompagnement pour visiter une agence ou faire une demande de services auprès d'une autre agence ; plaidoyer juridique et intervention liée au système ; développement des compétences d'emploi et la planification financière ; hébergement d'urgence ou maison d'hébergement pour femmes ; centres ou groupes de porte ouverte ; soins de santé ; travail de proximité ; aide spécifique à la culture ; services aux victimes ; groupes et classes de mentorat ; prévention de la violence et programmes éducatifs ; soins des enfants et transport ; dons de vêtements et autres articles ; art-thérapie et ludothérapie ; et programmes structurés qui viennent en aide aux enfants qui ont été victimes ou témoins d'abus (ex. ils ont vu leur père agresser leur mère). De plus, les programmes VFF canadiens ont plusieurs responsabilités au sein de leur communauté et aident les femmes, les jeunes et les enfants au-delà de leur mandat.

Utilisation de la technologie dans les programmes de VAW

De plus en plus, ces services ont une dimension technologique. La plupart des agences annoncent des services téléphoniques pour le public pouvant inclure une ligne détresse-secours disponible 24 heures par jour, sept jours par semaine et un service de téléimprimeur. La plupart des agences reçoivent également des demandes de communications volontaires ou non

sollicitées par l'entremise de la technologie comme les courriels, les textos, les sites Internet, Facebook, YouTube ou autre média social. Dans notre sondage 2013 « sur les pratiques d'utilisation de la technologie organisationnelle par les organisations œuvrant contre la violence faite aux femmes » plusieurs organisations VFF ont rapporté qu'elles fournissent des moyens technologiques sur place à leurs visiteurs, participants et résidents : 73 % ont une ligne terrestre et 40% fournissent l'accès à des téléphones cellulaires; 67% fournissent des ordinateurs de bureau et 27 % des ordinateurs portables ou tablettes; 35 % offrent des jeux vidéos et 4 % l'accès à des téléimprimeurs.

23 % des répondants au sondage fournissent l'accès Internet aux participants aux programmes VFF et à leurs visiteurs. 31 % fournissent l'accès Internet sans fil aux résidents de maisons d'hébergement et 17 % ont indiqué qu'ils fournissent aux participants/résidents/visiteurs un accès Internet indépendant du réseau réservé au personnel. Grâce à l'ordinateur et à l'accès Internet, les survivantes peuvent faire des demandes de logement, d'aide financière ou d'emploi tout en demeurant dans l'environnement sécuritaire de la maison d'hébergement ou auprès de l'organisation VFF. Ceci est important puisque l'homme dont elles sont victimes pourrait les contrôler ou les espionner en utilisant le même ordinateur qu'elles. L'accès à la technologie et à Internet peut également réduire le fossé numérique pour les femmes et les jeunes qui sont sans domicile fixe, qui ont de faibles revenus et dans les cas de harcèlement par la technologie et d'abus financier. Dans les cas où un abuseur ou un traqueur se présente dans un centre d'aide pour victimes de viol, ou autre agence de prévention de la violence, 60 % des programmes VFF qui ont répondu au sondage ont dit avoir des caméras de surveillance à l'extérieur de leurs édifices.

Protéger la vie privée et la confidentialité

95 % des programmes VFF qui ont répondu au sondage entreposent l'information reçue en format papier dans des classeurs. Environ 45 % conservent une partie de l'information sur un serveur interne, 15 % utilisent également un serveur hébergé, 19 % utilisent l'infonuagique (*cloud computing*) ou autre forme de stockage de données en ligne et 38 % utilisent cette information sur des ordinateurs personnels uniquement (non reliés à un réseau). De nombreuses organisations ont indiqué qu'elles mettent l'information en mémoire sur des clés USB et des disques à mémoire flash externes. Les répondants n'ont pas spécifié quels types de mémoire incluaient ou non l'information recueillie sur les femmes et les jeunes qu'ils aident.

Les pratiques d'utilisation des bases de données varient considérablement d'un programme VFF à l'autre. 51 % des organisations VFF qui ont répondu au sondage utilisent des bases de données pour recueillir et stocker de l'information sur les personnes (c.-à-d. les femmes et les jeunes qui demandent ou qui reçoivent des services ou de l'aide). Certaines de ces organisations continuent de compiler les informations sur papier et utilisent les bases de données pour soumettre des renseignements non identificatoires pour recevoir du

financement public. Certains recueillent de l'information de base dans une base de données pour des fins de statistiques uniquement. Un programme VFF a dit recueillir des statistiques stockées par une agence gouvernementale. Certaines agences ne documentent que les services fournis et d'autres créent un dossier électronique participant/client qui contient des renseignements personnels identifiables. Quelques programmes disent recueillir des statistiques qu'ils ne stockent pas mais soumettent à des agences gouvernementales.

Planification de la technologie de la sécurite

Les programmes VFF participent également à l'évaluation de la sécurité au sein de la population ainsi qu'aux réactions dans les communautés colocalisées et coordonnées avec d'autres secteurs et services comme la justice, les services sociaux et juridiques, la santé, la protection de l'enfance, l'éducation et autres agences sans but lucratif. Des exemples de telles collaborations incluent des équipes d'intervention auprès des victimes d'agressions sexuelles, d'incapacité, de violence conjugale, de comités d'observation des cas à haut risque et de décès et de comités de coordination au sein de la communauté. La technologie est utilisée de plusieurs façons dans le cadre de ces collaborations : avertir les membres de l'équipe qu'on a besoin de leurs services, recueillir des preuves, coordonner les services entre agences et partager l'information. Lorsque les travailleurs qui œuvrent contre la violence dans des agences VFF collaborent, ce qui implique une colocation, ils doivent parfois travailler sur place dans un poste de police ou dans un palais de justice plusieurs jours par semaine. La façon dont la technologie est utilisée dans ces situations peut affecter les droits à la confidentialité et à la vie privée de la femme qui recherche de l'aide. Il est primordial d'établir des limites claires dans l'utilisation de la technologie et l'accès à l'information électronique pour répondre aux mandats et protéger la vie privée et la confidentialité lorsque des programmes VFF collaborent ou travaillent dans un même lieu.

Alors que les programmes VFF utilisent la technologie pour améliorer leurs services d'aide, les travailleurs œuvrant dans le milieu sont plus souvent en train de planifier des stratégies de sécurité avec les femmes et les jeunes qui vivent les traumatismes générés par les abus de la technologie.

Ceci signifie que les survivants et les agences VFF ont maintenant affaire à des traqueurs, des abuseurs et des violeurs qui piratent les ordinateurs et les bases de données, qui menacent, qui personnifient, qui harcèlent par le biais des courriels et des médias sociaux et volent de l'information confidentielle par les réseaux sans fil et davantage. Voilà un petit échantillon d'abus technologique qui fait que leurs auteurs, dont le seul but n'est que de traquer, nuire ou tuer leur victime, arrivent à leurs fins. Cette réalité fait en sorte **qu'il est crucial pour les organisations VFF d'instaurer des pratiques organisationnelles de la technologie** visant à mieux protéger **la sécurité, la vie privée, l'identité et la confidentialité** des femmes, des jeunes et des enfants qu'elles aident.

Il est important que les agences VFF incluent l'utilisation de la technologie dans la planification de la sécurité des femmes et discutent de la façon dont les auteurs d'abus traquent, contrôlent, harcèlent et personnifient par le biais de la technologie. Les pratiques et les politiques de la technologie des agences doivent identifier et aborder toutes vulnérabilités touchant à la sécurité et à la vie privée qui pourraient être exploitées par l'abuseur afin d'avoir accès aux renseignements ou aux services de l'agence. Celle-ci doit prendre les précautions nécessaires pour s'assurer que toute forme de technologie est protégée et sécurisée adéquatement afin d'éviter que les auteurs d'abus aient accès à de l'information supplémentaire en vue de nuire davantage.

Pratiques organisationnelles de la technologie

Tous les programmes VFF font partie du secteur privé canadien et devraient évaluer l'impact sur la vie privée et la gestion du risque constant sur la vie privée pour s'assurer qu'ils utilisent la technologie de manière à mieux protéger les données identifiables et sensibles sur les femmes et les jeunes qu'ils aident. Les politiques et les pratiques des programmes et des agences doivent prendre des mesures extraordinaires pour protéger la confidentialité et l'identité des personnes à qui ils donnent des services ainsi que les données personnelles, identifiables et confidentielles qui ont été recueillies, stockées ou utilisées par des membres du personnel ou des bénévoles.

Toutefois, certains programmes VFF peuvent être confrontés à des obstacles importants lors de l'instauration de pratiques de la technologie solides portant sur la confidentialité, la vie privée et la sécurité. Trop de programmes VFF font face à un financement limité et instable. Ce ne sont pas tous les programmes VFF qui ont accès à du financement de base pour l'électricité et le chauffage, encore moins la sécurité et l'entretien de la technologie. Une minorité de programmes VFF ont du personnel formé en TI et encore moins ont un membre à temps plein ; la plupart du temps, les programmes VFF ont un petit contrat pour un consultant qui répond aux besoins en TI. Lorsqu'on leur demande, les principaux obstacles auxquels font face les organisations VFF lorsqu'elles veulent instaurer de telles pratiques sont les suivantes : manque de financement (69 %) et de temps (66 %); manque de connaissances et de formation sur les étapes de mise en place de moyens de sécurité de la technologie (62 %) ou sur les lois et les règlements concernant la vie privée et la confidentialité (46 %); la vitesse des changements technologiques et d'apparition de nouvelles technologies (58 %) et le besoin de plus d'exemples, d'échantillons et de modèles (59 %). Les organisations VFF qui ont répondu au sondage ont demandé plus d'information sur une gamme de politiques et de pratiques technologiques incluant les médias sociaux et le réseautage, la communication électronique, les téléphones cellulaires, la technologie de prestation de service, les dispositifs et services de repérage, les données et bases de données, la sécurité technologique, la vie privée et la planification de la protection de l'Identité.

Il n'est pas surprenant que ces agences veuillent développer et améliorer leurs pratiques en matière de technologie. Les agences de prévention de la violence organisent des évènements en ligne et hors ligne pour autonomiser les femmes et les enfants, pour appuyer les survivants, pour éveiller la conscience de la communauté dans la prévention et l'arrêt de la violence et honorer les femmes et les enfants qui sont morts des suites de la violence sexiste. Les évènements et les offres de formation qui étaient envoyés par télécopieur il y a quelques années, sont maintenant diffusés par courriel et affichés sur des sites Internet, Facebook ou autres pages de médias sociaux. L'inscription à des évènements est souvent faite sur des formulaires en ligne ou par courriel. Certains programmes VFF mettent sur pied des campagnes et des évènements en ligne ou par téléphone cellulaire. Lors de telles campagnes, les participants peuvent avoir à signer une pétition en ligne, faire un don, prendre et afficher des photos, afficher des articles dans les médias sociaux, faire des vidéos et les afficher, texter des messages pour une campagne, microbloguer (Twitter) sa propre expérience d'abus ou encore utiliser la technologie pour encourager les autres à faire de même. De nombreuses organisations VFF ont mis sur pied des programmes de développement de la compétence et de prévention de la violence en milieu scolaire basés sur la communauté et liés à l'âge. Les programmes VFF ont créé des applications d'intervention et de prévention, des vidéos, des jeux-questionnaires et des jeux pour aider les femmes et les filles à se sentir fortes. Lorsque l'on cherche à établir une communication par le biais de la technologie, il est important d'évaluer les conséquences possibles sur la vie privée, la confidentialité et la sécurité. Il est important de considérer les changements technologiques qui peuvent engendrer de nouveaux risques ultérieurement.

Il est important d'aborder le sujet de la vie privée et de la sécurité dans les pratiques de la technologie dans le cadre des programmes VFF parce que notre utilisation de la technologie peut augmenter ou diminuer les risques à la sécurité pour les femmes et les êtres qui leur sont chers. Par exemple, les politiques et les pratiques qui impliquent de retirer l'utilisation de la technologie peuvent avoir un effet d'asservissement auprès des femmes en donnant l'impression d'une forme de contrôle et de puissance. Le fait de demander aux femmes de ne plus utiliser les moyens technologiques n'est pas un gage de sécurité et peut même entrainer une augmentation des risques. Dans le cadre de notre mandat nous souhaitons encourager l'autonomie des femmes et des jeunes, leur autodétermination et leur droit à l'accès; Safety Net Canada ne recommande pas l'interdiction ou le retrait de moyens technologiques comme les téléphones cellulaires ou les ordinateurs. Nous encourageons plutôt toutes les agences de prévention de la violence à améliorer les connaissances et les habiletés des membres de leur personnel afin qu'ils puissent travailler de concert avec les femmes pour comprendre les risques et les avantages associés aux différentes technologies en matière de sécurité. Il est important que les participants et les résidents s'engagent à ne pas utiliser la technologie de façon à compromettre la vie privée, la sécurité, la confidentialité et la sécurité de l'identité des autres membres du personnel et des participants. Il est également très important de faire comprendre ce que cela implique.

Malgré nos bonnes intentions, il existe des pratiques de la technologie qui présentent plus de risques d'interception que d'autres. Sans mesures de sécurité (ex. le cryptage) la décision de stocker de l'information en ligne ou dans des bases de données électroniques ou de communiquer au sujet d'une femme ou avec elle par courriel ou texto peut augmenter les risques d'atteinte à la sécurité et à la vie privée. Les renseignements personnels recueillis et stockés en mode électronique, comme la nouvelle adresse et le nouveau numéro de téléphone d'une femme par exemple, peut avoir des conséquences inattendues et l'information peut facilement être interceptée et tomber entre les mains de son abuseur ou de son traqueur. Si les programmes VFF s'engagent à mettre fin à la violence faite aux femmes et autres filles, nous devons créer des politiques et des pratiques qui améliorent (et non pas le contraire) la sécurité, la vie privée, l'accessibilité, l'autonomie, la justice et les droits des femmes, des jeunes et autres victimes de violence familiale et conjugale, de violence sexuelle et de fréquentation, de traque et de harcèlement.

La technologie peut offrir des avantages incroyables aux organisations VFF et aux femmes et aux jeunes qu'elles aident. Les agences de prévention de la violence utilisent la technologie de manière innovatrice pour influencer directement la façon dont les communautés engagent la discussion dans le mouvement pour mettre fin à la violence envers les femmes et les enfants. Les programmes VFF doivent s'engager à ne pas utiliser la technologie de façon à augmenter les risques pour les femmes et les enfants qu'ils aident. Cela irait à l'encontre du mandat, de la mission et de la raison première pour laquelle les centres d'aide pour victimes de viol ont été créés.

Ce rapport traitent des pratiques organisationnelles reliées à l'utilisation courante de la technologie par les organisations VFF/de prévention. Il décrit et recommande des pratiques organisationnelles de la technologie qui amélioreront la sécurité et la vie privée des femmes, des jeunes et des enfants. Il met en évidence les questions à considérer lorsque vous mettez sur pied ou que vous renforcez les pratiques technologiques de votre programme VFF/de prévention; il inclut aussi des exemples et des scénarios qui peuvent aider à évaluer ces pratiques. Le but de cette ressource est d'aider les agences VVF **à augmenter leurs pratiques technologiques en matière de vie privée et de sécurité**.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS 2
EXECUTIVE SUMMARY 4
SOMMAIRE DE GESTION 9
TABLE OF CONTENTS 15
INTRODUCTION 17

USE OF TECHNOLOGY IN VAW AGENCIES: IMPACTS ON CONFIDENTIALITY, PRIVACY & SAFETY 19

SURVEYS: WHAT VAW AGENCIES TELL US 19
ANALYZING LAWS, POLICIES & REGULATIONS 21
INFORMATION PRIVACY, INFORMED CONSENT AND "SENSITIVE" INFORMATION 23
ONLINE COUNSELING AND SERVICES 25
MULTI-AGENCY COMMUNICATION & COORDINATION 27
OUTREACH, EDUCATION, PREVENTION, CAMPAIGNS 28
AGENCY TECHNOLOGY SECURITY PRACTICES 29
USE OF 3RD PARTIES TO MANAGE AGENCY TECHNOLOGY SERVICES & DATA 30

TECHNOLOGIES COMMONLY USED BY VAW AGENCIES: ENHANCING PRIVACY PRACTICES 32

PHONE TECHNOLOGY 32
EMAIL AND INTERNET TECHNOLOGIES 37
ELECTRONIC COMMUNICATION 40
LOCATION TECHNOLOGY 41
CAMERAS 41
WEBSITES 42
SOCIAL MEDIA & SOCIAL NETWORKS 43
ACCESSIBILITY & ASSISTIVE TECHNOLOGIES 43
DATA PRIVACY AND SECURITY 44
DATA COLLECTION ` 46
DATABASES 48

TABLE OF CONTENTS

APPENDIX A: SUMMARY REPORT: ORGANIZATIONAL TECHNOLOGY PRACTICES SURVEY FOR VIOLENCE AGAINST WOMEN PROGRAMS 50

APPENDIX B: SUMMARY REPORT: SURVEY OF ANTI-VIOLENCE WORKERS ON TECHNOLOGY ABUSE 71

APPENDIX C: PRIVACY, SECURITY AND CONFIDENTIALITY: DATABASE CONSIDERATIONS FOR VIOLENCE AGAINST WOMEN PROGRAMS 81

APPENDIX D: PRIVACY, SECURITY AND CONFIDENTIALITY: SOCIAL MEDIA CONSIDERATIONS FOR VIOLENCE AGAIST WOMEN PROGRAMS 100

INTRODUCTION

This guide provides examples of recommended promising organizational technology practices for Violence Against Women (VAW) programs**.** Its purpose is to best help VAW programs across Canada to protect the **safety, privacy, and confidentiality** of the women, youth, and children served. It also provides some scenarios to address some of the nuanced situations surrounding technology and organizational practice that VAW agencies must consider. In some sections we give a suggested policy. This *is suggested* and must be adapted for each program and community while keeping a feminist, women-centered and empowerment lens. VAW agencies are encouraged to use these examples, explanations and scenarios to **enhance privacy practices for technologies** commonly used by or in their agency or program (i.e. phones, databases, online, etc.).

"Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children" is one of three resources developed by Safety Net Canada (SNC) about the intersections of VAW, technology and privacy. "Assessing Technology in the Context of Violence Against Women & Children. Examining Benefits & Risks" and "Canadian Legal Remedies for Technology-Enabled Violence Against Women" complete our three reports.

All three resources should be used together and are guided by the philosophy that policies and practices should 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. We encourage VAW programs to adapt our suggested organizational policies to meet the diverse needs of their program while keeping the framework of safety, privacy and empowerment. This includes adapting policies and practices appropriately for inclusion of culture, local regional realities, and individualized needs.

Though our resources are developed primarily for VAW programs, many of the core elements of these recommended practices are strongly applicable to other victim serving programs. We also acknowledge that there are many other technologies that agencies use. It is still important to develop policies and practices about these technologies even if they are not included in this resource.

Realities of Safety Planning

Many VAW programs work with women and their children to develop an individualized safety plan and to help identify steps one might take that may increase safety[1]. Safety planning is an ongoing and active process because stalkers, rapists, and abusers may change abuse tactics and approaches at any moment. This is especially the case with technology. If an abusive tactic via

[1] Ministry of Justice, Safety Planning with Children and Youth: A toolkit for Working with Children and Youth Exposed to Domestic Violence, British Columbia 2011.

email doesn't provide the results that a perpetrator desires, (e.g. to have power and control, or to terrorize, harm, or coerce the woman, youth or child), then he has many more technologies to utilize. Abusers and stalkers choose a variety of techniques and tools for the purpose of power and control. Given this, it is important that safety plans are routinely discussed and adapted to meet the changing needs of women and children. While safety planning, it is important to consider technology as a benefit for women and children in addition to identifying and addressing risks.

VAW programs not only need to make sure that their current use of technology best anticipates and protects the safety, security and privacy of their participants, but they also should explore how expanding or changing agency technology use might increase accessibility in ways that further benefit a survivor's autonomy safety and privacy.

USE OF TECHNOLOGY IN VAW AGENCIES: IMPACTS ON CONFIDENTIALITY, PRIVACY & SAFETY

SURVEYS: WHAT VAW AGENCIES TELL US

In 2012 and 2013, Safety Net Canada distributed two surveys across Canada to programs supporting women and children fleeing and/or living with the effects of violence. The first survey titled "Survey of Anti-Violence Workers on Technology Abuse" canvassed Canadian anti-violence programs about how technology is being used to perpetrate violence against women in their community. The second survey, "Survey of Organizational Technology Practices" asked questions about what technology anti-violence programs are using and explored what policies and practices currently exist or are needed.

In this section, we will share the top three results of our surveys that address common practices of technology misuse by perpetrators and common organizational practices and policies regarding technology use by anti-violence workers across Canada. Summary reports of our surveys are available in the appendix for a closer look at technology and violence against women programs.

In our technology abuse survey, anti-violence workers responded to a list of eighteen common ways perpetrators use technology to harass, control, monitor, abuse and stalk women. They reported all eighteen tactics are forms of technology-enabled abuse used by perpetrators in Canada. The top forms of technology-enabled abuse by perpetrators against women and youth are:

Intimidation or threats via technology (98%)
Hacking into the survivor's email, social media and other online accounts (72%) or specifically hacking and monitoring Instant Messaging accounts (46%)
Impersonation: using email, online profiles or other technologies to pretend to be the survivor or someone she knows, such as a friend (69%).
Hacking into her computer to monitor her online activities and extract information (61%) or installing computer monitoring software or hardware e.g. spyware, keystroke loggers (31%)
Distributing or posting online pictures (60%) and videos (31%) of the woman/survivor without her consent. Using a hidden camera or her laptop's webcam to surreptitiously watch and record her without consent (31%)
Tracking her location via GPS device or other location service (including showing up everywhere unexplained (50%)

Misusing cell phones to track or monitor calls, location or other activities (49%)
Using landline phone (35%) or listening/recording devices (29%) to monitor conversations
Misusing caller ID to screen calls, or to spoof other phone numbers in order to call or text threats and abuse (44%)
Tampering with or destroying assistive technology, e.g. hearing aid, screen reader (10%)

Our survey of organizational technology practices asked anti-violence workers what technologies they use in VAW programs. The top technologies used in VAW programs are:

Desktop computers (98%) & Laptops (79%)
Multi-purpose photocopier and fax machines (91%)
Corded telephones & office phones (82%)
USB sticks (81%) & Memory Cards (41%)
Security/Surveillance cameras for outside buildings (60%) & video/digital cameras (51%)
Individual voicemail boxes (60%)
Mobile Phones: Basic Cell phone (54%) & Smart Phones e.g. iPhone, Blackberry (45%)
Cordless phones (48%)
Alert Devices: accessibility and safety devices that vibrate or/and flash lights when sounds go off like fire alarms, alarm clocks, door bells. (41%)

In terms of organizational technology policies and practices that address safety, privacy, confidentiality and security, the majority of programs had some policies for using technology when communicating with or about the women, youth and children and others who contact you or receive services and support. This includes using phones, fax machines and email. However, fewer than 50% of respondents had policies and practices in place around social media, video assistive technology, and use of personal technology by staff or participants.

Notably, 61% said their VAW program's work sometimes involved using equipment/devices both in office and offsite that are personally owned by staff, volunteers, or consultants. The most common devices used in these circumstances are laptops and netbooks, USB sticks, and mobile phones (basic and smart phones). While it is better for agencies to own these devices

and provide them to employees for work purposes, many VAW programs simply cannot afford to do this. Thus they rely on staff being willing to use personally-owned devices.

When asked "which organizational technology policy and practice standards would your VAW program most would like to see developed to address and protect safety, confidentiality, privacy, personal identity and security of workers, women and children?" The top picks were:

Social media and networking (76%)
Electronic communication (69%)
Technology safety and privacy planning (60%)
Mobile phones and other devices (58%)
Technology use in counseling and service provision (56%)
Data and databases (55%)
Location tracking, mapping, sharing, tagging devices and services (52%)
Identity protection planning (50%)

Our Canadian survey coincided with the National Network to End Domestic Violence (NNEDV)'s survey on technology use and policies. Not surprisingly, the findings from our two surveys are similar to those from NNEDV. One major difference is that a higher proportion of Canadian anti-violence programs rely mostly on paper participant files than the electronic files used in US programs. This may be because many Canadian non-profit VAW programs don't have annual line-item funds written into grants that address the bricks and mortar of implementing and maintaining sufficient security and privacy protections on the personally identifiable information (PII) of participants. These VAW programs are aware of some of the privacy risks and given limited resources, decide that paper in a locked filing cabinet is sufficient.

The results of the two surveys informed our recommendations of organizational technology practices for VAW programs that enhance privacy, confidentiality, safety and security.

ANALYZING LAWS, POLICIES & REGULATIONS

The privacy and confidentiality policies and practices of VAW agencies are impacted by a variety of federal and provincial/territorial laws, policies and regulations. Examples include:

- Privacy obligations under federal and/or provincial law.

- Confidentiality provisions for a type of VAW program or worker in a particular jurisdiction.[2]
- Confidentiality and/or privilege obligations and other provincial/territorial laws governing the practices of credentialed licensed professionals such as lawyers, social workers, medical doctors and therapists.[3]
- Regulations created by funders for audit purposes.
- Laws and regulations dictating timeframes that a VAW program should retain information in a participant's record for specific purposes such as protecting the future rights of the participant to appeal agency decisions[4] or, keeping records that help document the sexual abuse of a minor to provide the option for that survivor to press charges later as an adult before the statute of limitations ends[5].
- Mandatory reporting laws and determining the specific information VAW programs must share and may not share when reporting suspected child abuse or making other mandatory reports.

Sometimes these laws, policies and regulations seem to conflict. *For example,* it is considered a best practice that VAW programs collect the least amount of information from a participant that is needed to deliver services. It is also considered a best privacy practice for the VAW program to dispose of any personally identifiable information as soon as it is no longer needed to deliver services. However sometimes, funders or professional regulatory bodies ask VAW programs to keep records for many years past the date when the information is needed to provide services. How do VAW programs be accountable for best protecting the sensitive and private information of the women and children who are at risk when they receive conflicting messages on whether to retain or delete some personally identifiable information.

These laws influence the ways that agencies use technology. *For example*, VAW programs that wish to be accredited may have to purchase an electronic database in order to meet accreditation standards. Though electronic databases pose privacy risks to survivors, agencies must make the decision to purchase a database or lose service delivery contracts. VAW programs sometimes find themselves in conflict between not using certain technologies because they are neither confidential nor secure or abiding by funder requirements.

In this guide, we take into account laws that are protective of privacy and confidentiality in ways that supports safety. Some of the recommendations may not be consistent with the current requests or recommendations of an outside funder or related profession. We

---

[2] Example: Personal Information Protection Act. April 2013 http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01)

[3] Federation of the law societies of Canada http://www.flsc.ca/; Canadian Association of Social Workers www.casw-acts.ca; Canadian Association of Social Worker Education www.caswe-acfts.ca

[4] Personal Information Protection Act. April 2013 http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[5] Ruebsaat, Gisela. Records Management Guidelines: Protecting Privacy for Survivors of Violence. BC Association of Specialized Victim Assistance and Counselling Programs and BC/Yukon Society of Transition Houses. 2006.

encourage VAW programs to talk with funders or colleagues about mandatory technology use by funders and identify the increasing safety, privacy and confidentiality risks to the women, youth and children you serve.

INFORMATION PRIVACY, INFORMED CONSENT AND "SENSITIVE" INFORMATION

Canada has a number of federal and provincial/territorial laws that define privacy obligations of private sector organizations that collects and stores personally identifiable information. These laws include but are not limited to the Personal Information Protection and Electronic Documents Act, BC's Personal Information and Privacy Act, Quebec's An Act Respecting the Protection of Personal Information in the Private Sector and the Personal Information Protection Act of Alberta. Under these laws, "organizations are required to develop internal policies that give effect to the principles contained in Canadian private-sector privacy legislation"[6]. Canadian VAW programs, whether standalone or part of a larger multi-purpose agency, are responsible for the protection of any personal information they collect and keep.

Promising Practices:

- VAW programs must identify, assess and develop good privacy practices, policies and procedures
- Train employees regularly on privacy risks
- Appoint a privacy officer who takes the lead on privacy management and issues
- Ensure that the VAW program goes through a process to identify "privacy related obligations and risks" including with technology and staff practices, each time "before they launch new products or services"[7].
- To comply with this properly, VAW programs need to understand the privacy ramifications of different technologies they use to communicate or collect personally identifiable information. Given other regulations, this is especially pertinent when personally identifiable information becomes part of a record that a VAW program decides to keep about an individual.

Notice, Transparency and Informed Consent

Most VAW programs know that they need to be vigilant about providing robust notice, ensuring transparency, and training staff and volunteers about their role in ensuring that any consent to collect or share a person's information is informed and not coerced or pressured. VAW program staff should consider that informed consent involves being as specific as possible for the

[6] OIPCA, OPCC, OIPCBC (2012, April) Getting Accountability Right with a Privacy Management Program, p. 10.
[7] OIPCA, OPCC, OIPCBC (2012, April) Getting Accountability Right with a Privacy Management Program, p 1.

current situation, and thus it is ongoing conversations between staff and an individual woman over time.

Informed consent, like safety planning, is not something that is obtained once with an abuse survivor. A woman may consent to collection or sharing of information one day, and then two days later, realize there is a new safety risk and she wants to withdraw her consent. This is the reality of the lives of survivors of sexual violence, domestic violence, stalking and abuse. Fundamentals to informed consent are**:**

- She has a right to say no repeatedly and for any reason. This may impact the types of services she can receive.
- She should never be refused services simply because she does not consent to VAW programs' collection or storage of her personally identifiable information.
- VAW program staff should have a practice of always asking for permission.
- Be transparent about what you'd like to add to her record. For example, "this was an important conversation, I'd like to add this to your participant file because …"
- Show her any records you keep about her and, if relevant, her children.
- Ask her if there is anything she'd like to have corrected.
- Let her know who will or might see her personal information within the VAW program or broader organization. Explain why this occurs.
- Tell her others won't be able to see her information without her consent.
- Take her opinions seriously if she disagrees with one of your practices.
- Provide her the upfront and ongoing option of anonymity whenever feasible (e.g. on crisis lines and in person).

Informed Consent to Release of Information

VAW program participants must provide time-limited informed and written consent in order for a program to collect and share personally identifiable information. Consent must include the fact that the participant can withdraw her consent at any time. To inform consent, anti-violence workers must ***Practice:***

- Being transparent about what your VAW program will do with her data and how it will be used.
- Informing women of their right not to disclose any information.
- Notifying her that services may not be conditioned on release of information.
- Explaining what will you document.
- Tell her where her data is going to be stored and how it will be secured.
- Sharing who has access to her information and who might be able to access this information in the future.
- Having a clear process for release or sharing of information.
- Letting her know how her personally identifiable information will be destroyed and when.

- Being clear about what are the risks to her privacy, confidentiality and safety if your VAW program collects her data. This is especially true if your agency uses electronic databases.

Knowing the potential life-threatening risks faced by the women and children who ask VAW programs for support, it is imperative that our use of information technology does no harm. VAW programs should never use a technology (email, Internet-connected computer, e-fax and database) to collect or store information about a woman if we can identify ways that her privacy and safety is better protected by using a different technology or simply keeping that information in a locked filing cabinet.

ONLINE COUNSELING AND SERVICES

There are compelling reasons for VAW programs to offer online service provision (OSP) to participants. OSP, otherwise known as online advocacy, online counseling, e-services, is an emerging method for providing services to people who have been abused, stalked, or sexually assaulted. OSP can include any online contact with survivors, their children or other support persons, for the purposes of providing support/counseling, information, referral, safety planning, or prevention/risk reduction. The technologies used vary and might include websites, email, internet relay services (audio, text, and video), VOIP (internet phones), listservs, chatrooms, blogs, social networking sites, or instant messaging.

Survivors are increasingly seeking information and real-time support online. Potential benefits have been documented. OSP can open up the possibility of serving survivors who may have limited access to your agency's traditional in-person and phone services, such as women who have communication or mobility disabilities, live in rural and remote communities and/or are youth. The potential risks are also well documented and include possible decreased safety and confidentiality for participants, possible decreased effectiveness of services, issues around creating accessibility and a host of technical and resource-related issues such as a loss of internet connection. Regardless of why your agency provides OSP, VAW programs must be transparent about limits and risks and set up an alternative plan, for example, in case you are disconnected. If you are considering or assessing the possibility of OSP here is a table of outlining ***Promising Practices:***

Assess your Readiness	• What is your technology staffing/capacity? • Develop a good communication plan. • Are other resources needed? • Is OSP likely to achieve the desired outcomes of your VAW program? • What are the costs/risks vs benefits? • Is OSP allowed under current grants?

	• How will your program ensure confidentiality?
Develop a Plan	• Decide where you will start? • Do they align with your VAW program ethics? • Limit staff who provide OSP. • Start with existing participants. • Choose methods of communication (asynchronous or real-time; email, webform, individual or group chats, open or closed, IM webcam, relay). • Have passwords. • Prepare for session time outs and loss of internet connection. • Have a way to evaluate OSP. • Prepare for any liability issues.
Conduct Technology Safety Checks with Participants	• Be transparent about confidentiality and privacy risks. • Ask survivors whether they are in a safe place and using a safe computer/device. • Ask what type of technology they are using such as VOIP, calling from cell phones or cordless phones. • Safety plan with survivors around disconnection and risks of OSP.
Accessibility	• Identify if the method of OSP is accessible. • Ask if your OSP platform can be more accessible.
Create Policies, Regularly Assess & Adapt	• How can staff respond to OSP demands from survivors? • How and where is the data stored? • Is OSP meeting the needs of women accessing your program? • Are you ready to expand?
Evaluate Effectiveness	• Are participants' satisfied? • Where there any technical issues? • Is OSP accessible? • Were you able to maintain the confidentiality and privacy of participants?
Test Your Security	• Test OSP system for intrusion and hacking often. • Were any communication intercepted? • Install Firewalls and Anti-virus programs.
Confidentiality	• Keep up to date with changes to the OSP system.

	• Plan around what kind of information will be shared between staff and survivor. • How will confidentiality breeches affect your program?
Stay Informed about New Technology	• What are the ways new technology can impact survivors? • Should you update the technology you are using? • How can your program switch over safely and seamlessly? • Can all staff be trained?
Creating Resources	• Develop policies and practices. • What are the lessons learned? • Share resources and lessons with other VAW programs. • Apply for grants and secure funding for ongoing OSP development and maintenance.

Suggested Policy:

Confidentiality can be harder to maintain through an online service provision (OSP) process for a number of reasons. The risks of OSP must be fully understood by the provider, and conveyed to the survivor who will be participating in OSP. OSP can include e-mail based counseling, chat-based (instant messaging) counseling, web-based messaging, video-based counseling, or some combination of those technologies with telephone or face-to-face interactions. Staff will take steps to assure, to the extent possible, that OSP, if done, is accomplished in as secure a fashion as possible, and with the full understanding of the survivor of the risks of such counseling.

MULTI-AGENCY COMMUNICATION & COORDINATION

VAW programs participating in multi-agency communication and coordination committees such as sexual assault response teams, disability response teams, domestic violence response teams, high-risk and fatality case review committees and community coordination committees must develop practices about technology use. Technology is being used in many ways during these collaborations, including to alert team members that they are needed, collect evidence, coordinate inter-agency services, and to share information. When anti-violence workers at VAW agencies do collaborations that involve co-location, this will sometimes mean that they work onsite at a police station or court house several days a week. How technology is used in these circumstances can enhance or undermine the confidentiality and privacy rights of woman seeking support. Clear boundaries in technology use and access to electronic information are critical to meeting mandates and protecting privacy and confidentiality when VAW programs

collaborate or co-locate. ***Promising Practices*** around technology use must be in place for the purpose of consent to share personally identifiable information:

- Did all committee members obtain a release of information?
- Who has access to the information?
- What are the risks to women's personally identifying information and privacy?
- What are the risks when her personally identifiable information is located within another agency?

Suggested Policy:

Confidentiality of survivor information that is requested from the program by any other person or agency will not be released unless there is a specific informed, time-limited release (waiver) from the survivor whose information is sought to be shared. The survivor should be required to execute separate, specific, informed, time-limited releases as necessary to release information at varying times during the provision of services.

OUTREACH, EDUCATION, PREVENTION, CAMPAIGNS

Anti-violence agencies deliver a variety of outreach, education, prevention activities and anti-violence campaigns via technology. Technology is being used to:

- Organize events online.
- Engage the community in preventing and ending violence by sharing information.
- Honour the women and children who have died as a result of gender-based violence.
- Announce events and training dates.
- Post videos and pictures.
- Create online or mobile phone campaigns.

There are benefits for online outreach and campaigns. VAW programs such as Metrac and the YWCA have created online games and apps that engage and educate survivors about safety. Online campaigns also reach a wider audience at a faster pace.

However, there are several dilemmas that can arise. There have been common unanticipated consequences of VAW program initiated campaigns. VAW programs participating in online outreach and campaigns must develop practices around confidentiality and privacy. Some scenarios to consider are 'what happens when a survivor discloses personally identifiable information on your online campaign webpage?' or 'if a survivors' picture and/or name was posted or included without consent?'

AGENCY TECHNOLOGY SECURITY PRACTICES

There are many ways agency security can be compromised via technology. This section addresses risks to agency technology and includes basic practices for VAW programs.

RISKS TO AGENCY TECHNOLOGY	PROMISING PRACTICES
Virus	• Install anti-virus software on all computers. • Keep anti-virus software up to date and renew. • Use Firewalls. • Have a plan in place for if a virus is not detected by anti-virus programs.
Keyloggers/Spyware	• Post safety alerts on agency websites that computers may not be safe. • Safety plan with women about using safer computers when visiting the agency website. • Do not keep personally identifying information on computers that can be monitored/connected to the internet. • Do not download attachments or click on links from unknown sources or that look suspicious.
Bad Passwords	• All staff must have separate passwords. • Passwords should be a mix of letters, numbers and symbols. • Passwords should not include any agency information. • Staff should not share passwords. • Have one administrative password for the designated agency administrator to access the agency computer system/network in case accessing the system is needed.
Hacking, Packet Sniffing and Interception	• Do not store personally identifiable information on any computer connected to the internet. • Encrypt all data. • Install Firewalls. • Have a plan in place for if your agency's computer system is hacked sniffed and data is intercepted.
Spoofing and Impersonation	• Set up code words with survivors. • Do not share personally identifying information.

	• Safety plan ways to confirm the identity of the caller.
Access/Storage Destruction	• Have one or minimal staff have access to IT administrator controls and passwords. • Back up data regularly. • Encrypt data. • Use Firewalls and anti-virus programs.

USE OF 3RD PARTIES TO MANAGE AGENCY TECHNOLOGY SERVICES & DATA

This section addresses the use of third parties to manage agency technology or provide agency services. Suggested practices are provided.

3RD PARTY AGENCY TECHNOLOGY	PROMISING PRACTICES
Online Survey System	• Read and understand the privacy policies and ownership of data rights of the 3rd party managed technology. • Understand the privacy laws of the jurisdiction the 3rd party technology is hosted in. • Do not have one password for all users. • Uncheck 'capture IP address' function. • Do not ask for any personally identifying information from survey respondents. • Only collect aggregate data. • Inform respondents of the purpose of the survey/evaluation and how the information will be used. • Delete all survivor data from the system as soon your agency is finished collecting data.
Webinar / Conference Calls	• Read and understand the privacy policies and ownership of data rights of the 3rd party managed technology. • Understand the privacy laws of the jurisdiction the 3rd party technology is hosted in.

	• Inform callers that you are recording the call/webinar and where it might be posted. • Do not ask for any personally identifying information. • Remove all recorded calls/webinars from the webinar program as soon as possible. • Maintain participants confidentiality when asking/responding to questions.
Cloud Computing	• Read and understand the privacy policies and ownership of data rights of the 3rd party managed technology • Understand privacy laws of the jurisdiction the 3rd party technology is hosted in. • Know what country the cloud is hosted in and the laws that agency information is privy to. • Encrypt data. • Know who is connected to the Cloud and how it works.
VOIP providers for phone lines	• Read and understand the privacy policies and ownership of data rights of the 3rd party managed technology. • Understand the privacy laws of the jurisdiction the 3rd party technology is hosted in. • Provide women with alternate ways to contact you in case you are disconnected. • Consider alternative practices when calling 9-1-1 in case you are disconnected and emergency services cannot call back.
Offsite Data Storage	• Read and understand the privacy policies and ownership of data rights of the 3rd party managed technology • Understand the privacy laws of the jurisdiction the 3rd party technology is hosted in. • Know who has access to your data. • Have legal written contracts about ownership of data, filing cabinets, hard drives etc. • Create policies about portable data storage such as USB keys and removable hard drives.

TECHNOLOGIES COMMONLY USED BY VAW AGENCIES: ENHANCING PRIVACY PRACTICES

PHONE TECHNOLOGY

Voicemail Greetings

Suggested Policy:

The organization will decide the best information to include in the outgoing message, attempting to provide basic technology safety information. Teams will determine the appropriate information to include in individual staff outgoing messages, attempting to provide safety information to callers on how staff can most safely reach them.

Promising Practices:

- When appropriate, staff may want to include in their outgoing messages: "please leave a number where it is safe for us to call you, and also let us know if it is safe to leave a message."
- Staff might develop a list of outgoing message options to share with teams.
- Use hard to guess passwords.
- Let callers know that perceptions of voicemail being confidential is misleading if perpetrators can easily hack passwords.

Leaving Voice Mail/Answering Machine Messages

Suggested Policy:

If returning the call of a survivor or possible survivor, staff will attempt to access the situation and leave either no message or a limited message, unless they have been told by the survivor/caller that it is safe to leave a message.

Promising Practices:

- When attempting to leave a message staff may choose to leave minimal information or hang up and reconsider options.
- Think through possible brief responses.
- If the potential survivor has not given explicit permission to leave a message at safer number, then staff are encouraged to talk to colleagues to better assess safety and privacy issues.

Voice Mail Passwords

Suggested Policy:

Staff will attempt to use secure passwords and will change them regularly. Teams will determine how often voice mail passwords should be changed depending on the sensitivity of messages each team receives.

Promising Practices:

- At a minimum, staff should change their voice mail password once per year. Voice mail passwords should not be the same as their extension or "1234". When teams need access to joint voicemail boxes, teams can determine more secure passwords that are not easy for the public to guess.

Staff Cell Phone Use and Sensitive Information

Suggested Policy:

Your agency must determine the appropriate use of personal and agency owned mobile phones for use in communicating sensitive information, striving to not share identifying information about potential victims/survivors.

Promising Practices:

- Staff that travel may find times when they cannot avoid sharing some sensitive information between staff on a mobile phone. Whenever possible staff should attempt to anonymize information or at least not share last name and full contact information.
- On very rare occasions when staff might need to use a cell phone to call a possible victim/survivor, staff should tell her that they are using a cell phone and suggest that they not use last name or other identifying details.
- The organization can consider providing staff with safer cell phones, such as newer more confidential cell phones.

Staff Cordless Home Phone Use and Sensitive Information

Suggested Policy:

Staff discussing sensitive work information from a home phone should make every effort to use a traditional "corded" phone, rather than a cordless phone. Staff should also ensure that there is no one in proximity to overhear their conversation.

Promising Practices:

- If staff must make or receive a call in which identifying or sensitive information about a woman might be discussed, they should use a traditional corded phone since cordless phones can be intercepted by neighbour's baby monitor, cordless phones, and radio scanners.

Incoming Calls on Mobile Phones or Cordless Phones

Suggested Policy:

When staff believes a caller may be using a mobile or cordless phone and the call includes sensitive information, as appropriate and possible the staff will attempt to provide basic information about mobile phone privacy to callers, always respecting the caller's decisions about their privacy needs.

Promising Practices:

- Staff should consider how to become attuned to cell and cordless phone use. For example: a mobile phone may be in use if staff can hear background or road noise, or the connection seems to come and go. A cordless phone may be in use by the caller if staff can hear some interference on the line such as a radio station or another conversation.
- If staff believe a caller is on a mobile or cordless phone and the discussion includes sensitive information, staff will attempt to ask the caller if they are on a mobile or cordless phone, mention that these phones are not completely private, and ask if the caller would prefer to call back on a regular "land line" or corded phone.

Caller ID & Blocking on Organization Phone/Fax/TTY Lines

Suggested Policy:

The organization will block Caller ID on all outgoing phone lines and/or have a policy about blocking individual outgoing phone calls. The organization will designate staff to periodically test the Caller ID blocking and work with the phone service provider to add permanent Caller ID blocking to all office and cell phone lines.

Promising Practices:

- To ensure that Caller ID blocking remains staff can call someone who has Caller ID to test each line, including the TTY and Fax lines. Since phone company changes can inadvertently remove Caller ID Blocking, testing should occur at least once per year or more frequently if the organization changes phone service providers.

- If permanent Caller ID blocking is not in place, staff are encouraged to use *67 to block Caller ID of any regular or mobile phone being used to call a possible survivor or an unknown participant.

Spoofing

Suggested Policy:

Teams will determine the most appropriate time, applications and methods for staff to use spoofing applications as needed.

Promising Practices:

- If a staff is concerned that their blocked line can be 'unblocked' or blocking technology is not available in your community, using spoof technology may be an option to provide an alternative Caller ID.
- If it is determined that you will be using spoofing technology to call back a survivor let her know what number to expect to see on her Caller ID.
- Choose a Caller ID number that is generic and will not raise suspicions with an abuser.

Anonymous Call Rejection (when receiving a call with Blocked Caller ID)

***Suggested Policy**:*

Teams will determine the most appropriate methods to return a call to someone who has "Anonymous Call Rejection", attempting to not unblock the line when potentially calling a survivor. Staff may use the phone company operator to connect a call when necessary, even if it incurs a moderate charge. Since there are various electronic call screening packages that can accompany Caller ID, teams will determine how much information to provide to an electronic call screening system.

Promising Practices:

- If staff might be returning a call of a survivor, they can use a variety of options to reach someone with Anonymous Call Rejection such as requesting that an operator connect the call, or using a phone card that has been tested and does not show the organization number in Caller ID.
- When calling a possible survivor and staff encounter an electronic screening system they may chose to provide limited information. For example, some privacy manager programs ask staff to state their name and enter their phone number before ringing through to the recipient while the caller is on hold. In this case, staff might choose to only say "I'm returning your call from this morning". If they privacy manager asks staff to enter their phone number, staff may chose to enter 555-1212 or 123-456-7890 rather than entering the organization's phone number into a possible survivor's phone system.

- When staff encounters Anonymous Call Rejection or other screening systems, staff are encouraged to discuss options with colleagues and/or attended several technology safety trainings.

Text Messaging

***Suggested Policy*:**

Staff will discourage survivors from using text messaging to communicate with them, and will attempt to provide basic information about the risks of text messaging confidential information, while respecting the survivor's decisions about her privacy needs. Teams will determine policies around personal mobile phones to text message survivors.

Promising Practices:

- If staff should receive a text message from a survivor, they will respond in a way that avoids sharing any confidential information in a responsive text message.
- Staff will make reasonable efforts to delete confidential text messages and call history from phones.
- If staff use smart phones or other portable devices that receive e-mails and/or text messages, they will make reasonable efforts to delete e-mails and confidential information from the device.

Incoming and Outgoing Faxes

Suggested Policy*:*

Departments and teams will include safety information on all outgoing fax cover sheets including information such as Caller ID, confidentiality, and, when appropriate, a request to remove the cover sheet and fax header. Teams will determine the safest way to provide information regarding safety and privacy to people requesting faxed resources. When faxing sensitive information or possibly faxing a survivor, staff will attempt to contact the recipient before sending the fax. When reasonable, staff will attempt to remove any sensitive incoming faxes from the fax machine as soon as possible to increase the privacy of the information.

Promising Practices:

- Departments and teams might include a line on fax cover sheets encouraging the fax recipient to remove the cover sheet and cut off the fax header when forwarding sensitive faxed information. This could be a checkbox that is only checked when appropriate.

TTY and Relay Services

***Suggested Policy**:*

The organization will designate one or more point persons for TTY and Relay Services. If the organization has a TTY device, the point person(s) will ensure that the equipment is maintained and repaired and that all appropriate staff are trained on using the TTY device. The point persons will also provide information to all staff about relay services.

Promising Practices:

- Designated staff should make sure the TTY is working properly on a regular basis. This may include making a TTY call to another organization with a TTY to make sure that it is working properly. The TTY device should be tested or used for calls at least once a month to know that it is working correctly.
- The point person(s) might want to invite an external speaker to the organization to provide training to all staff on using a TTY device.
- Staff should delete all histories the TTY device might save after the completion of each TTY call.
- If the TTY device prints or displays messages of incoming calls/messages, the TTY device should be a in a secure and/or private area. If the TTY device is equipped with a password to prevent messages from printing overnight, then the password should be used and known by appropriate staff persons.

EMAIL AND INTERNET TECHNOLOGIES

Organizational Website

***Suggested Policy**:*

The organization will put brief information about Internet Safety on every page of their website, and provide live links to more detailed Internet Safety information. The organization will not post any staff/organizational email addresses on their websites. If the organization chooses to allow visitors to contact the organization via the website, it will provide interactive "web forms" (or another comparably safer web-based method) for those visitors to use. The organization will attempt to provide as much Internet safety education and informed consent mechanisms as possible and reasonable to those choosing to contact the organization. This information will be reviewed and updated annually (at minimum) to ensure it addresses safety risks of emerging technologies.

Promising Practices:

- Since Internet search engines and other websites can link visitors to any page of the VAW program website, the brief Internet safety piece included on every page of the website should always alert website visitors to issues of "computer tracking" and safer computers and provide links to more detailed information.
- The organization and teams should screen any web-based Internet safety pieces with the goal of providing enough information for a survivor to be alerted to potential safety risks while minimizing information that might inform abusers on ways to misuse technology.
- To best decrease safety risks to external website visitors, the organization's interactive web forms (or another comparably safer web-based method) should alert users to technology safety risks that promote informed consent by: asking the visitor to choose one or more safer methods for the organization to contact them, and by providing relevant information that increases a website visitor's ability to make informed decisions about safety risks of such contact.

Increase Website Privacy

***Suggested Policy**:*

The organization will support the privacy of staff by providing notice and gaining consent prior to posting information about staff in electronic files on the website or posted directly on web pages. Teams that develop materials and content for the web will provide notice and gain permission from staff whose names or photos might appear on the website. Whenever reasonable the organization will support staff who prefer not to have their name or photo on the organization website or in a document that might be posted to another website.

Promising Practices:

- Supervisors could be responsible for collecting permission from staff to have their name and/or photo in the organizational report, organization website or other website documents prior to its electronic posting.

Internal Organizational Email

***Suggested Policy**:*

Staff will attempt to keep identifying information about victims/survivors out of emails. Whenever possible, staff will not send or forward emails containing identifying information about a possible victim/survivor without first removing identifying details. Whenever possible, staff will attempt to assess risk and choose the safer methods to share potentially identifying and confidential information about possible victims/survivors.

Promising Practices:

- Staff may decide to share important, but non-identified information in emails. Participant-identifying information such as full name and phone number may be more safely shared in-person, or on a (secure, not cell or cordless) phone, or within voicemail.
- Staff may chose to delete identifying victim information before forwarding an email to another staff person or consultant, and communicate the identifying information in another, more private manner.
- Staff working with consultants should create practices regarding the sharing of sensitive information with consultants. These practices may need to take into account inter-organizational communication policies and the security of various systems used by consultants. These practices should be communicated to all relevant impacted staff.
- To help all staff manage sensitive emails, teams are encouraged to share suggested alternative practices for communicating potentially confidential and identifying information.
- Other electronic communication such as through Instant Messages or emails delivered to mobile phones or tablets should follow the included email privacy provisions, as the safety and confidentiality risks are essentially the same.

Replying to External Emails

Promising Practices:

- External email coming through an agency web form gives women (or other website visitor) the ability to share the safest way to reply. When a woman has had the opportunity to complete a mini "safety plan" on the web form, it is important to respect her desires for response method, whenever possible.
- When responding to women, it may be best to delete the entire original message (do not include the original message in the reply) in case others read the response.
- If women find an agency email address and do not access the organization through the web form (where they can provide the safest way to reply), staff may want to respond to those emails from survivors with a short message referencing the crisis line number for information (We received your email and are happy you reached out to us. The best place to get the resources you mentioned can be reached 24 hrs a day and toll free at 123-456-7891).
- Create a brief sentence about email privacy and safety issues at the top or within the signature/footer of some or all-outgoing emails. Teams may also choose to include a web address to additional technology safety resources in some or all outgoing emails. Such outgoing emails may include auto-response emails, broadcast alerts, etc.
- Staff or email accounts that receive many unsolicited external emails, including from survivors, might chose not to use auto-response emails when they are out of office.

Encouraging Privacy though Listservs

Suggested Practices:

- Staff may need to occasionally send gentle reminders to listserv particpants about removing identifying information such as victim name, phone, or highly identifying details.
- Listserv signup information and initial greeting information might include general information about confidentiality practices and the risks of interception by others, including abusers.
- Staff with privacy concerns may choose not to have their name listed as an author on a document being shared outside of the organization.

ELECTRONIC COMMUNICATION

Maximize Security of Electronic Communication: Email, Instant Messaging, Text Messaging, Using Web Cameras and Video Conferencing

Suggested Policy:

Teams will determine policies about electronic communication including electronic communication through personal use of electronic devices to best protect the confidentiality, privacy and safety of all survivors.

Promising Practices:

- All forms of electronic communication will be password protected.
- Passwords should not be the staff member's name, project name, or other easily guessed word. When possible, passwords should include at least one number and a combination of letters.
- Staff may decide to share important, but non-identified information electronically. Participant-identifying information, such as full name and phone number, may be more safely shared in person, or on a secure (not cell or cordless) phone, or within voicemail.
- Staff may chose to delete identifying victim information before forwarding communication to another staff person or consultant, and communicate the identifying information in another, more private manner.
- To help all staff manage sensitive electronic communication, staff members are encouraged to share suggested alternative practices for communicating potentially confidential and identifying information.
- All electronic communication such as through Instant Messages or emails delivered to smart phones or tablets should follow the included email privacy provisions, as the safety and confidentiality risks are essentially the same.

- When responding to survivors, it may be best to delete the entire original message (do not include the original message in the reply) in case others read the response.
- Teams may choose to create and include a brief sentence about electronic communication privacy and safety issues in some or all-outgoing emails.
- If staff should receive electronic communication from a survivor, they will respond in a way that avoids sharing any confidential information in a responsive message.
- Staff will make reasonable efforts to delete confidential messages and call history from (personal) phones.
- If staff uses smart phones or other portable devices that receive e-mails and/or text messages, they will make reasonable efforts to delete e-mails and confidential information from the device.

LOCATION TECHNOLOGY

Promising Practices:

- Educate staff of safer ways to use technology that have potential location tracking risks.
- Educate and safety plan with survivors about safer ways to use technology that have potential location tracking risks. Location tracking devices can be placed in cars, toys, computers, mobile phones, accessories and more.
- Learn how to turn off location sharing/tracking services on mobile phones and computers, strip geotags off photos, and opt-out of checking in and sharing location through social networks and then educate survivors.
- Discuss privacy options for location sharing services.
- Do not ban or take away technology as this practice is disempowering as survivors may need technology in case of emergency or to connect with their support networks.
- Strategize with survivors and law enforcement about removing location tracking devices before doing so as it can alert perpetrators.

CAMERAS

Suggested Policies:

Teams should develop policies to address retention of video footage and use and purging of camera images. Policies should address how agencies will limit access to the images, the camera and any media (memory card, videotape, hard drive) and ensure that they are not lost or stolen.

Promising Practices:

- A log should be kept of all instances of access to, and use of, recorded material.
- Agencies should maintain the security of any system or computer used to view camera or video feeds.
- Have strong computer and system firewalls, keeping anti-virus and anti-spyware programs current, encrypting the camera feed/transmission, and requiring each person to have a unique user name and password for the computer/system and for the camera/video account.
- All passwords should be changed at the very minimum, one year or every time there is staff turnover.
- Agencies and partnerships should keep video footage only for the shortest time necessary to address victim safety or other security issues.
- Be upfront and transparent at the time of intake about video camera recording.
- Have notification, signs and information to tell participants accessing services that they are being taped or viewed by cameras.
- Review relevant laws relating to privacy, consent and video/audio recording before purchasing, installing and using cameras to record or view participants.

WEBSITES

Promising Practices:

- Have global safety alerts on all of agency web pages to indicate that computer activities may be monitored.
- Have a quick escape button that takes visitors to a neutral website such as one to look up the weather.
- Provide alternative ways for visitors to receive information such as phone numbers.
- Design agency websites so that they are accessible and able to be read by screen readers and/or enlarge text.
- Do not post staff contact information on websites. Instead use a web forum that can prompt visitors to specify how they would like to be contacted.

SOCIAL MEDIA and SOCIAL NETWORKS

Safety Net Canada acknowledges that there are many important considerations to think through before and agency commits to social media/network(s). Please see Appendix D "Privacy, Security and Confidentiality: Social Media Considerations for Violence Against Women Programs" for more detailed information.

Promising Practices:

- Assess the capacity and readiness of your agency to use social media.
- Discuss what social media/networks align with your agency ethics, missions and values.
- Have plans around liability issues especially around privacy breaches.
- Ensure there are policies developed around posting of personally identifying information by agency and/or survivors.
- Assess the accessibility of your social media/network application.
- Safety plan with women, youth and children about participating in your agency's social media/network.
- Have plans for if perpetrators threaten and harass agency staff and/or survivors through your social media/network site.
- Ensure that agency social media/network privacy and security settings are up to date and check regularly.

ACCESSIBILITY & ASSISTIVE TECHNOLOGIES

Promising Practices:

- Ensure that your program is accessible to women of all abilities.
- Purchase new equipment and devices to ensure accessibility such as flashing lights for doorbells, text screen/inputs for intercoms, TTY machines.
- Determine practices around communicating through relay operators.
- Safety plan with survivors about alternative ways to communicate if they are being monitored or their assistive device has been tampered with or destroyed.
- Train and schedule staff who know how to use assistive technology to communicate with survivors.
- Set up code words or phrases with survivors in the case of impersonation.

DATA PRIVACY AND SECURITY

Minimize Collection of Sensitive and Identifying Electronic Victim Information

***Suggested Policy**:*

Staff will determine how much identifying information is appropriate and necessary to collect about survivors and attempt to minimize the amount of sensitive or identifying information collected whenever possible. Agencies are encouraged to remove identifying or sensitive information as soon as the information has served its purpose.

Promising Practices:

- Programs are encouraged to collect and electronically enter the minimum amount of information necessary to effectively achieve the goals of service. For example if age is helpful, staff could document age range or age, but not date of birth. If the province/territory is relevant, but the exact city is not needed to respond to a brief phone call, then province/territory should be the only information documented electronically.

Purge or Remove Sensitive and Identifying Electronic Victim Information

***Suggested Policy**:*

Each program will determine how long identifying or sensitive information is maintained electronically, attempting to keep the minimum amount of information to be effective. Teams will attempt to remove or purge narrative details about victims/survivors as soon as possible, leaving only the minimum amount of information to meet grant requirements or effectively achieve project goals. Programs may choose to share some information in-person, via a paper note, or by phone, rather than enter sensitive information into an electronic database. Programs that collect or maintain information for external projects or databases will design them with privacy and safety in mind, but may need to maintain different information than other organizational projects.

Promising Practices:

- Initial staff may collect and document more detailed information that is helpful to the responding program staff member, but not necessary to maintain after the request is resolved. All staff are encouraged to continually remove identifying and sensitive victim information, storing only the minimum amount of information to meet the project goals. For example, narrative details may be helpful in responding to an initial request, but only the categories of information sent might be needed once the request was resolved.

Minimize Access to Sensitive and Identifying Electronic Victim Information

Promising Practices:

- When appropriate, a VAW program in a multiservice agency might share minimal details of a call or request with other members of a department or across the organization without sharing identifying information such as name. A victim or survivor name may only be relevant to the responding staff person.

Maximize Security of Electronic Victim Information

***Suggested Policy**:*

The organization will attempt to maximize the security of all electronic information, but especially any possible victim/survivor information. The agency will attempt to ensure maximum internal and external data security, but must assist in the security effort by minimizing the collection and storage of highly sensitive electronic information.

Promising Practices:

- Staff who are concerned about entering certain highly sensitive information are encouraged to enter less identifying information into an electronic system and use a more secure means to share the identifying details. The organization will support staff who assess privacy risks and will offer several mediums (phone, paper, database).

Maximize Security of Email and Electronic Security

***Suggested Policy**:*

Staff will attempt to use secure passwords and will change them regularly. Teams will determine how often email and/or database passwords should be changed depending on the sensitivity of information being received or collected. When any staff member leaves the organization, passwords for shared email and database systems containing sensitive information will be changed

Promising Practices:

- When staff leaves the organization, supervisors could list all of the databases and shared accounts that a staff person was accessing so that the appropriate staff members can change the passwords.
- Passwords should not be the staff member's name, project name, or other easily guessed word. When possible, passwords should include at least one number and a combination of upper and lowercase letters.

DATA COLLECTION

Minimize Collection of Sensitive and Identifying Victim Information

Suggested Policy:

Only the minimum information necessary to provide services to the survivor will be gathered and maintained.

Promising Practices:

- Evaluate intake forms and processes to ensure that only the minimum information necessary is requested to provide effective services.

Notification to the Survivor of the Program's Confidentiality Obligation

Suggested Policy:

The survivor will be notified of the program's obligation to maintain confidentiality of the survivor's information, the limits of confidentiality (both under the law and through the challenges of technology, if used), and the right that she has to choose to waive confidentiality under certain circumstances. The survivor will be notified of the program's record retention and destruction policy.

Promising Practices:

- Have a short handout ready to read to/give to a survivor that outlines the program's obligation regarding confidentiality of the survivor's information and the survivor's rights regarding her confidential information.

Securing Confidential Client Information

Suggested Policy:

The program will take necessary steps to secure all confidential survivor information, whether maintained electronically or on paper. The program will maintain and follow telephone and computer safety policies to help to safeguard such confidential information.

Promising Practices: For Securing Paper Information

- Security measures should be in place to protect all electronic and paper records.
- No individual staff, volunteer or consultant with the program may have access to any personal, identifying survivor information unless the individual has signed a confidentiality agreement with the program.

- Paper records that include individual, identifiable survivor information should be stored in locked filing cabinets in locked rooms which is secure at all times. Access should be limited to specific personnel and as necessary to perform a job role or with a demonstrated "need to know". Whether there is a "need to know" includes an emergency situation.
- Files that are accessed should be signed "out" when viewed and "in" when returned.
- Any documents that contain personally identifying survivor information should be shredded as soon as the need for such document or information has passed. The retention and destruction of documents will be accomplished on a timeline and through a process defined in the organization's document retention and destruction policy.

Promising Practices: For Securing Electronic Information

- Electronic records should be properly secured electronically, with alphanumeric passwords and, where appropriate, user access levels that are limited to the minimum access level necessary to perform a job role. If electronic backups or paper copies of any program records are stored off site, they should be protected and purged in the same manner and within the same time limits as information stored onsite.
- Use alphanumeric passwords and change them frequently.
- If a program chooses to have an information intake system, and a user forgets a password, the user should (select 1 or more options):
    - Use paper files until they are able to reach the system administrator for a new password;
    - Log in with the permission of another user with a similar access level under that user's account, carefully document the anomaly, and then have both users' passwords changed within 24 hours or as soon as they are able to reach the system administrator;
    - Contact the on-call system administrator (if the program has one).
- Electronic records will be purged in a manner consistent with the program's record retention and destruction policy.
- To the extent possible, electronic records of survivor information will be maintained on a computer that is not connected to the Internet.
- Test your security by having a trusted and skilled consultant or security firm test the security of the organization's network and data protection procedures.

Information Outflow: Protecting Information from Being Released without a Waiver

***Suggested Policy*:**

Confidentiality of survivor information that is requested from the program by any other person or agency will not be released unless there is a specific informed, time-limited release (waiver) from the survivor whose information is sought to be shared. The survivor

should be required to execute separate, specific, informed, time-limited releases as necessary to release information at varying times during the provision of services.

Promising Practices:

- In order to provide the highest level of confidentiality protection possible, the process should provide for a written release only upon informed consent that includes all of the following:

    - A review with the survivor of the specific information that is to be released;
    - The risks and benefits of releasing the confidential information;
    - The reminder that the program staff and the survivor may not be able to control what happens to the information once it has been released to the outside agency, and any anticipated further disclosures that may occur;
    - The purpose for which the information is to be released;
    - The duration for which the release is valid (the specific number of hours, or days, not to exceed 30 days);
    - The method by which the information will be released (e.g., phone call, copied documents sent by mail, e-mail, etc.) and the risks of such method of communication; and
    - Specific designates agencies or individuals to whom the information will be released.

- The survivor may withdraw her release at any time, and the withdrawal is effective as soon as it is given. Oral withdrawals are as effective as written withdrawals, although an oral withdrawal should be reduced to writing as soon as possible.

DATABASES

The previous suggested policies and promising practices also apply to databases. Safety Net Canada acknowledges that there are many important considerations to think through before selecting a database as a way to store participant data. Please see Appendix C "Privacy, Security and Confidentiality: Database Considerations for Violence Against Women Programs" for more detailed information.

Suggested Policy:

The program will not provide any personally identifying information regarding any survivor to a database that is accessible by any individual or agency outside of the program.

Promising Practices:

- The program may share non-personally identifying data in the aggregate regarding services to participants and non-personally identifying demographic information in order to comply with funder reporting, evaluation, or data collection requirements. A survivor will not be asked to provide a waiver or release in order to share her information in a database that is accessible by any individual or agency outside of the program.

APPENDIX A

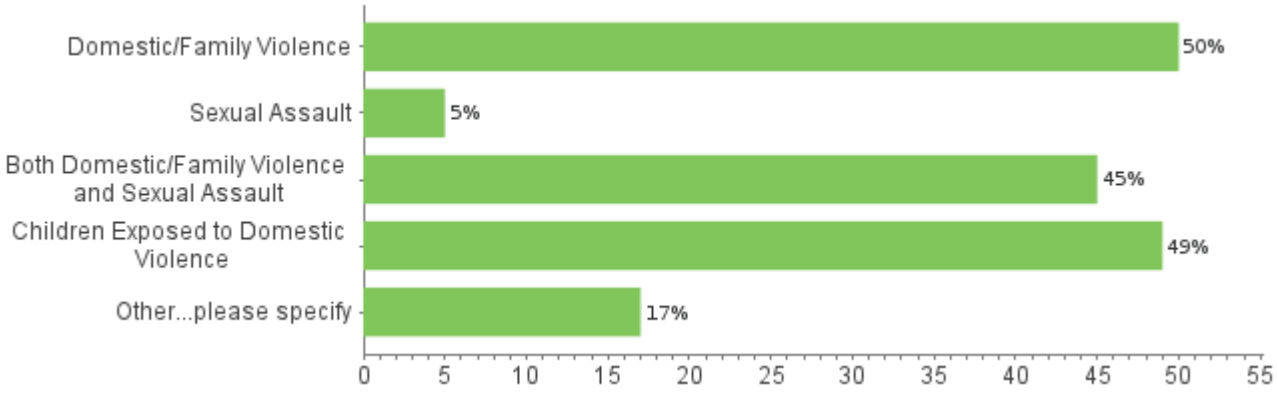
Summary Report: Organizational Technology Practices Survey for Violence Against Women Programs

Section A: Background Information about your VAW Program

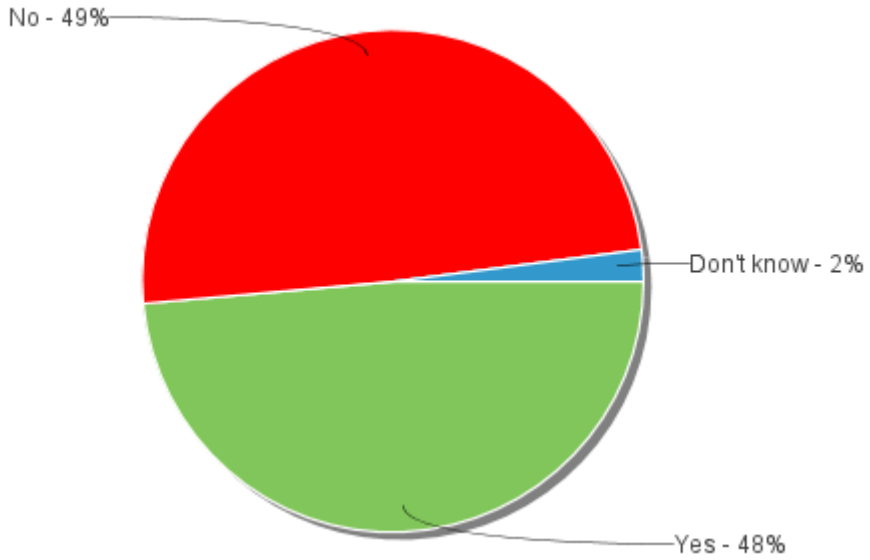
1. Canadian Province/Territory where you work:

Response	Chart	Percentage
Ontario		5%
Quebec		25%
Nova Scotia		7%
New Brunswick		1%
Manitoba		5%
British Columbia		46%
Prince Edward Island		0%
Saskatchewan		2%
Alberta		5%
Newfoundland and Labrador		1%
Northwest Territories		2%
Yukon		1%
Nunavut		0%

2. Type of VAW Program

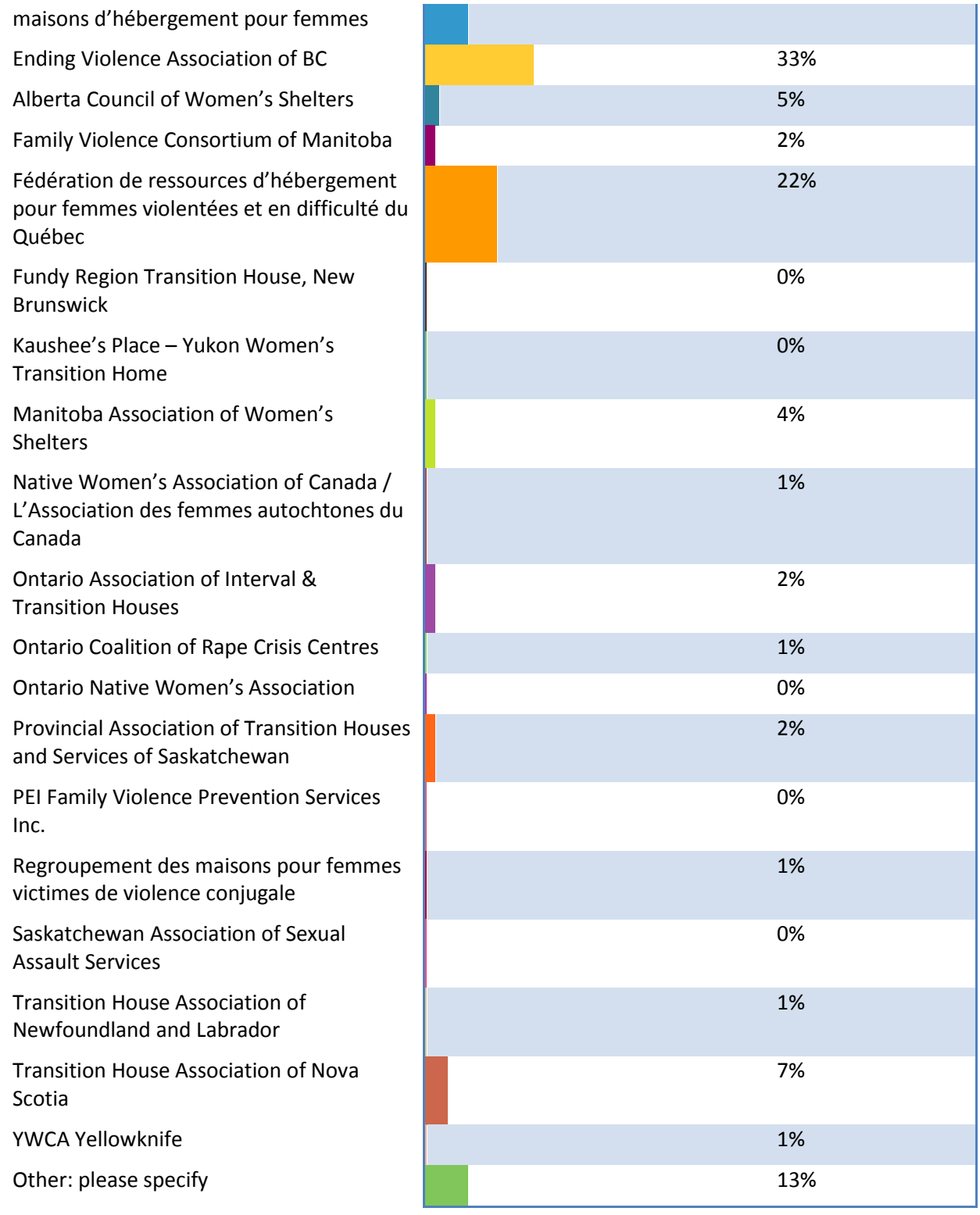


3. Is your VAW program part of a larger multi-service organization?

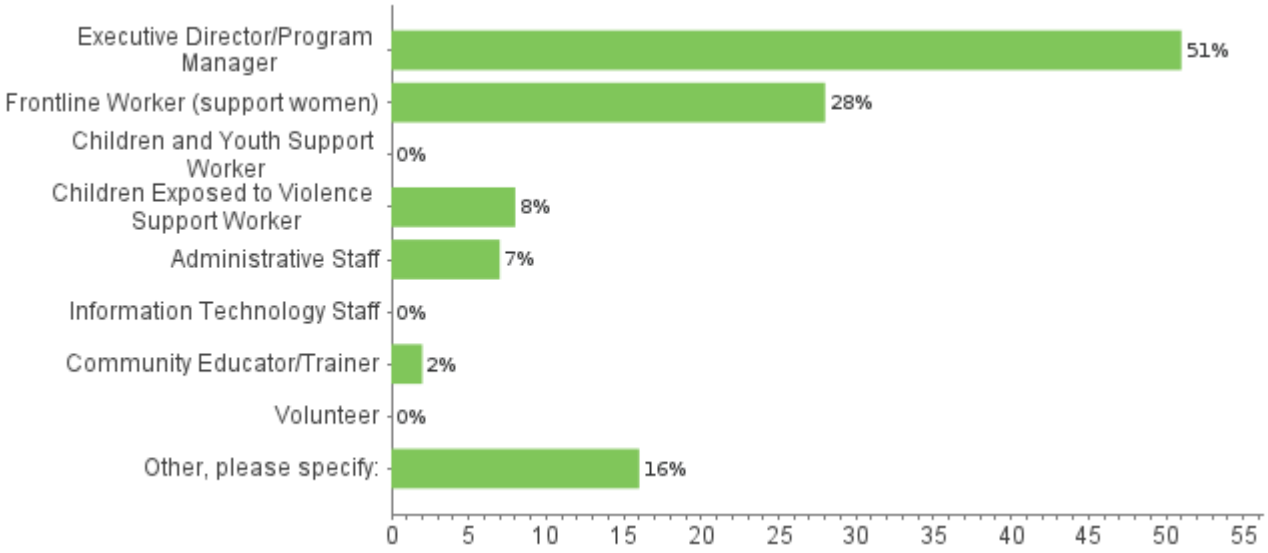


4. Is your VAW program a member of any of the following provincial, territorial, Aboriginal, or national association?

Response	Chart	Percentage
BC Society of Transition Houses		29%
Canadian Association of Sexual Assault Centres/Association Canadienne des centres contre les agressions à caractère sexuel		2%
Canadian Network of Women Shelters and Transition Houses / Réseau canadien des		13%


maisons d'hébergement pour femmes
Ending Violence Association of BC
33%
Alberta Council of Women's Shelters
5%
Family Violence Consortium of Manitoba
2%
Fédération de ressources d'hébergement pour femmes violentées et en difficulté du Québec
22%
Fundy Region Transition House, New Brunswick
0%
Kaushee's Place – Yukon Women's Transition Home
0%
Manitoba Association of Women's Shelters
4%
Native Women's Association of Canada / L'Association des femmes autochtones du Canada
1%
Ontario Association of Interval & Transition Houses
2%
Ontario Coalition of Rape Crisis Centres
1%
Ontario Native Women's Association
0%
Provincial Association of Transition Houses and Services of Saskatchewan
2%
PEI Family Violence Prevention Services Inc.
0%
Regroupement des maisons pour femmes victimes de violence conjugale
1%
Saskatchewan Association of Sexual Assault Services
0%
Transition House Association of Newfoundland and Labrador
1%
Transition House Association of Nova Scotia
7%
YWCA Yellowknife
1%
Other: please specify
13%

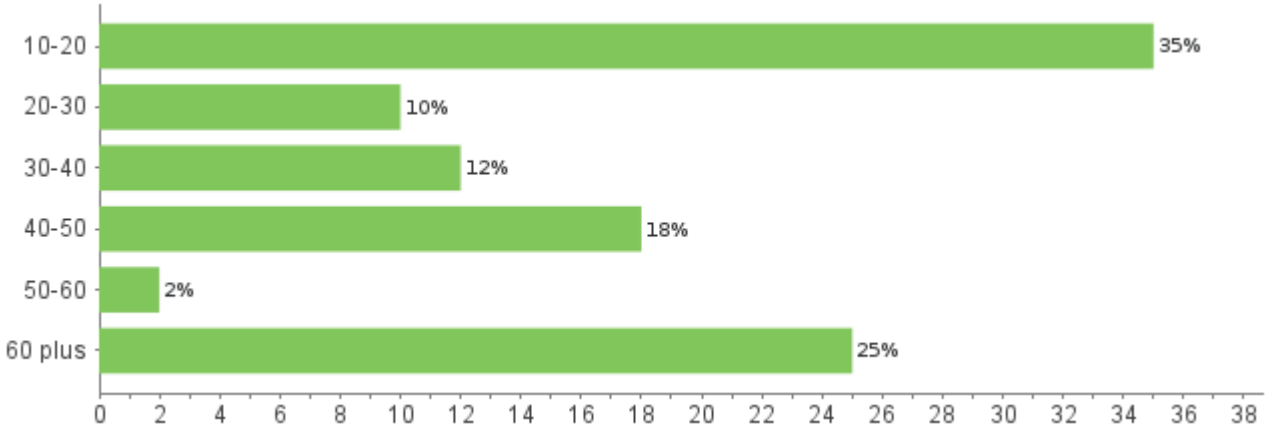
5. What best describes your role in your agency?



6. How many paid staff work in your VAW program/s?

The responses ranged from 1-225 paid employees.

If your VAW program/s is in a larger multi-service agency approxiamtely how many paid staff work in your entire agency?



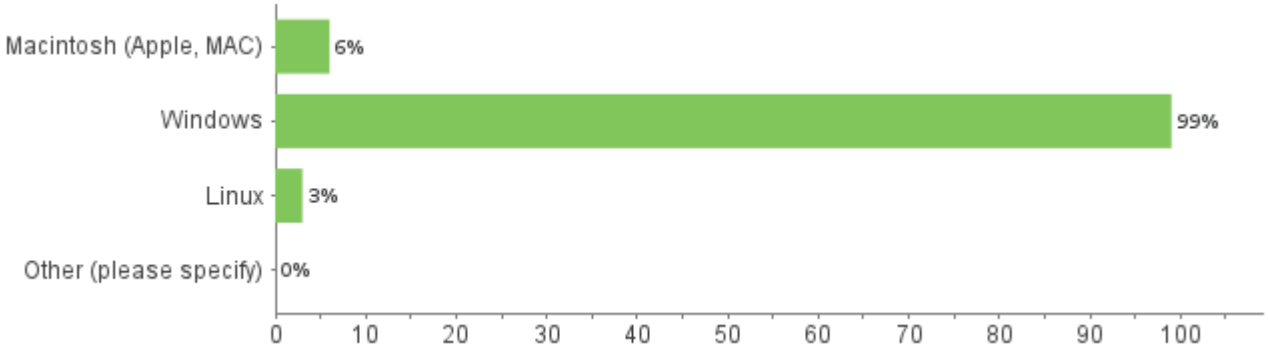
7. If we have questions about your survey response, may we contact you via email? If yes, please provide an email address:

67 respondents provided their email address.

Section B. What Types of Technology Does Your VAW Program Use?

You may need to ask your coworkers some of these questions. Your answers to this section will provide the VAW sector with a better understanding of the types of technology that our Canadian VAW Programs are using. We are interested in learning about technology: owned and maintained by your program/organization and personally owned by staff, volunteers and consultants who do work for your VAW program.

8. What Computer Operating Systems (OS) does your organization/VAW program use?



9. What types of Equipment/Devices does your VAW program use?

Response	Percentage
Laptops (and Netbooks)	78%
Desktop Computers	99%
Mobile Tablets (iPad, Android, etc)	13%
Computer Server	36%
USB sticks	81%
Memory Cards (often used in digital cameras)	41%
Portable or desktop backup drives	28%
Office Phone System	85%
Individual voicemail boxes	60%
General voicemail box accessed by several people	31%
Corded Phones	85%

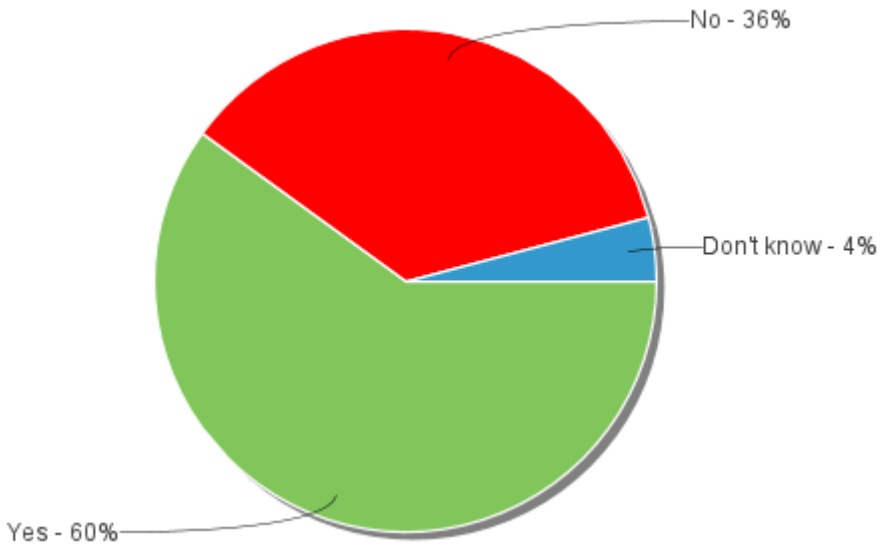
Cordless Phones	47%
Basic Mobile / Cell Phones (phone plan has calls, texts, voicemail)	55%
Mobile/ Cell "Smart" Phones like iPhones, Blackberry, Android that can access the Internet	44%
Pagers	5%
Multi-purpose copier and fax machine	88%
Stand alone fax machine	35%
Web camera (plug-in device or built into a computer/mobile phone or tablet)	29%
Security/Surveillance Camera for inside buildings	23%
Security/Surveillance Camera for outside buildings (entrances, parking, etc.)	59%
Video / Digital camera (take photos at events, create videos, etc.)	50%
Cameras (to record evidence of abuse)	21%
Alert Devices (accessibility and safety devices that vibrate or/and flash lights when sounds go off like fire alarms, alarm clocks, door bells)	41%
TTY / TDD (Teletypewriter or Telecommunications Device for the Deaf)	9%
Video phone (often used to communicate with sign language interpreters)	1%
Other (Please specify)	9%

Other:

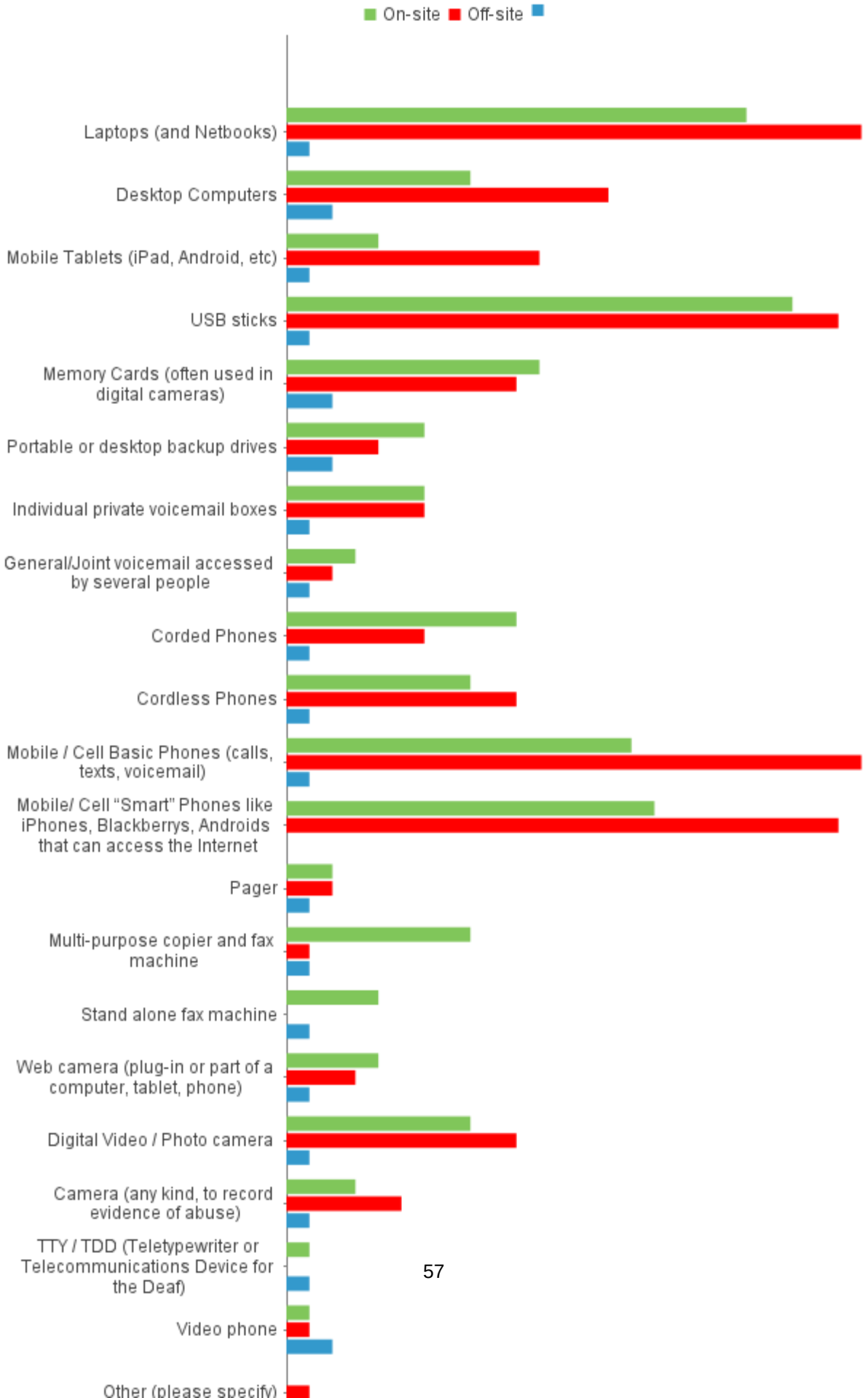
#	Response
1.	Panic buttons for staff. Press button and RCMP respond.

2.	panic button alarm systems
3.	appareil pour personnes sourdes à venir
4.	life line for staff security
5.	Lifeline Security Pendants x 3
6.	système de sécurité pour l'immeuble
7.	Projecteur

10. Does your VAW program's work ever involve using Equipment/Devices that are personally owned by staff, volunteers, or consultants?



11. If yes, which technology personally owned by staff, volunteers or consultants is used onsite (in VAW program offices) or/and offsite (at the person's home and elsewhere) for VAW program work?


On-site
Off-site
Laptops (and Netbooks)
Desktop Computers
Mobile Tablets (iPad, Android, etc)
USB sticks
Memory Cards (often used in digital cameras)
Portable or desktop backup drives
Individual private voicemail boxes
General/Joint voicemail accessed by several people
Corded Phones
Cordless Phones
Mobile / Cell Basic Phones (calls, texts, voicemail)
Mobile/ Cell "Smart" Phones like iPhones, Blackberrys, Androids that can access the Internet
Pager
Multi-purpose copier and fax machine
Stand alone fax machine
Web camera (plug-in or part of a computer, tablet, phone)
Digital Video / Photo camera
Camera (any kind, to record evidence of abuse)
TTY / TDD (Teletypewriter or Telecommunications Device for the Deaf)
Video phone
Other (please specify)

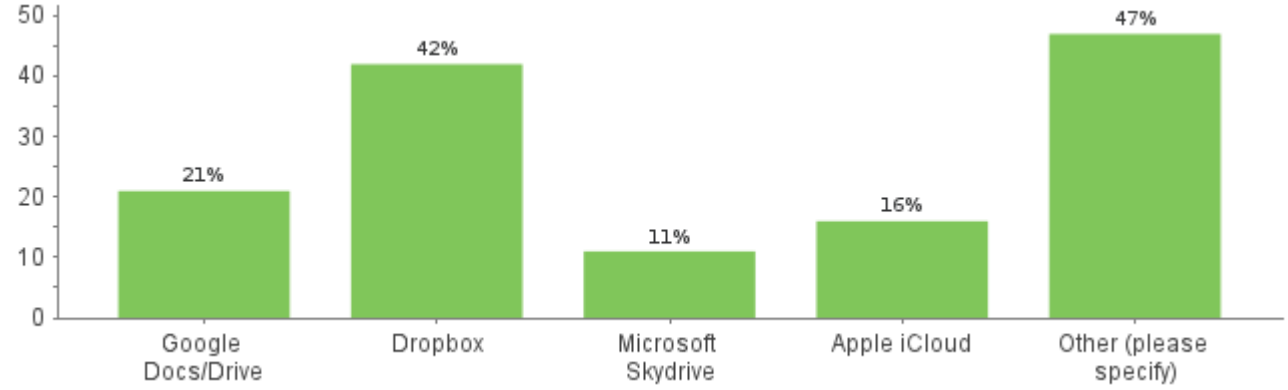
12. How do you store the information that your VAW program collects (financial files, participant records, etc.)?

Response	Chart	Percentage
Paper files in cabinets		95%
Individual computers only (not a network server)		37%
In-house Server (a computer server located inside your offices. Server stores some of the VAW program files or applications and provide access to them via your network.)		45%
Third-party Hosted Server (a server located offsite that you rent space on. Other people own the server and maintain your network security and access.)		15%
Cloud Computing or other Online Data storage		17%
Other (please specify)		8%

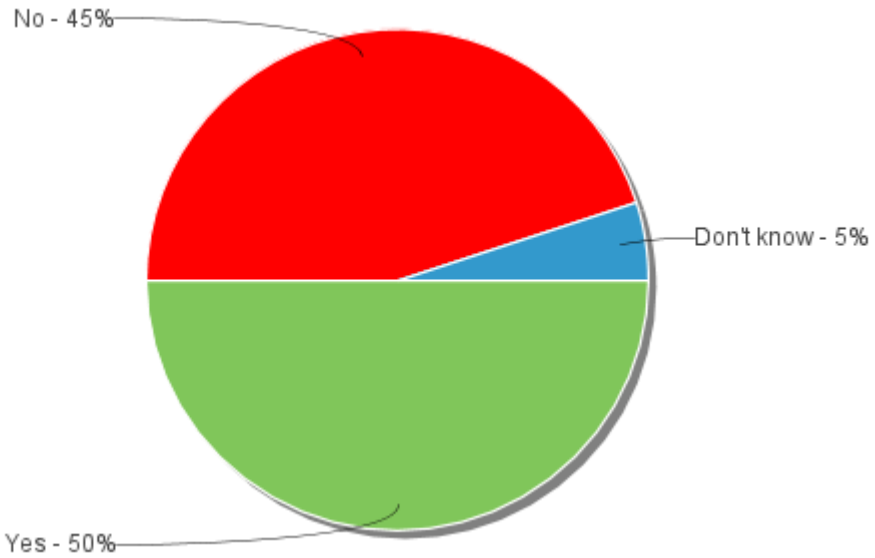
Other:

#	Response
1.	thumb drive
2.	data sticks
3.	moving to a server this year
4.	stats on flashdrives
5.	considering networking, have a nonfunctioning netweorker server, would like to have off site financial data storage
6.	Clé USB

13. If you use cloud computing or other online data storage to edit or store files, what do you use?



14. Does your VAW program (or broader organization) use databases to collect and store information about clients? (by client information, we mean information about women, youth and children who request and/or are provided services and support).



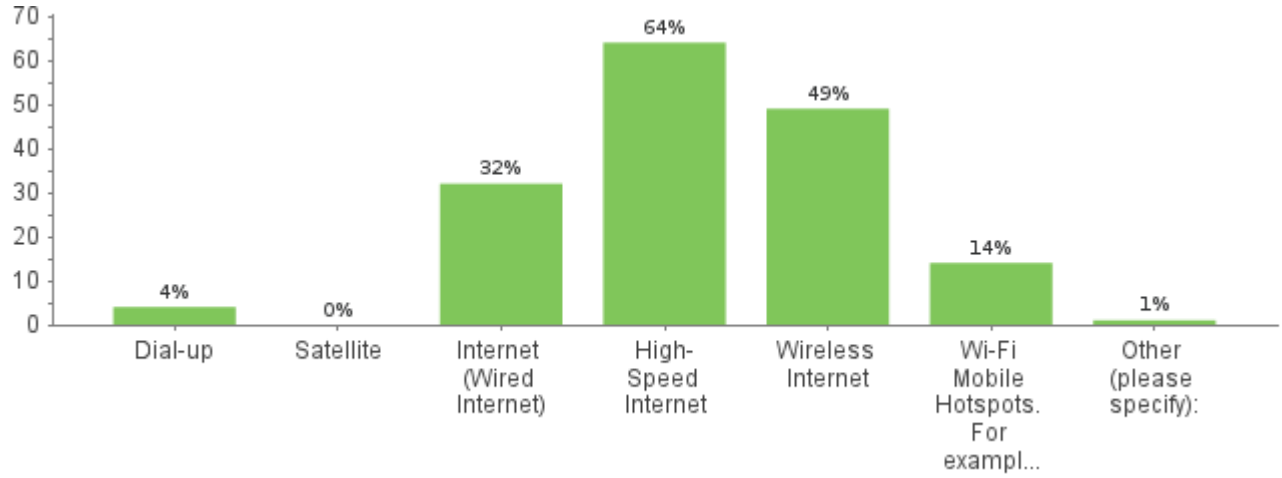
15. If yes, please describe the database/s your VAW program and/or organization uses to hold information about participant?

The 38 response(s) to this question can be found in the appendix.

Response	Chart	Percentages	Count

Databases Used		26%	10

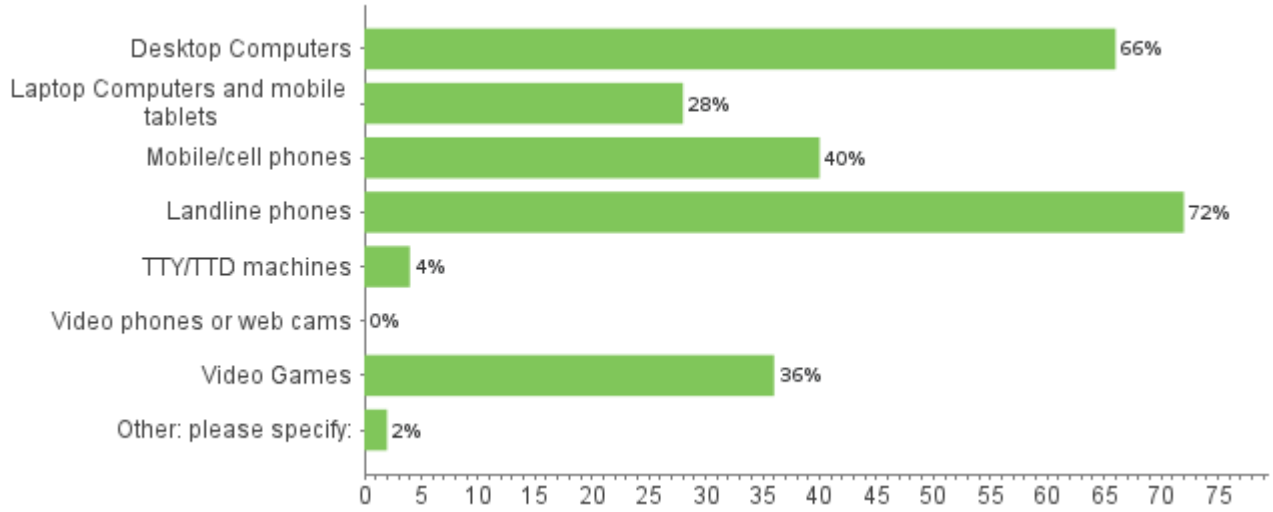
16. How does staff access the internet?



17. How do participants or visitors to your VAW program access the Internet?

Response	Chart	Percentage
We do not provide any Internet access to participants or visitors.		33%
We provide Internet access to people who visit or receive VAW program services.		22%
We run a women's shelter or transition/interval house, and only provide wireless Internet access for shelter/house residents.		30%
We provide participants/residents/visitors with access to an Internet network that is separate from our staff/employee network?		17%
Other		11%

18. Does your VAW program own or rent technology that you let participants use onsite or offsite?



19. Which online and social media platforms does your VAW program use?

Response	Chart	Percentage
Website		73%
Blog or Vlog (video online blog)		9%
Online discussion forum or chat rooms		3%
Facebook		44%
MySpace		1%
Google+		13%
Tumblr		0%
Pinterest		3%
Reddit		0%
Twitter		20%
YouTube or other video sharing site		13%
Flickr or other photo sharing site		1%
Online games or virtual worlds		3%
None		20%
Other (please specify):		4%

20. Why does your VAW program use social media?

Response	Chart	Percentage
Education/Awareness		91%
Fundraising		53%
Connect with other advocates, agencies, and allies		53%
Outreach to women		64%
Not sure		5%
Other (please specify):		7%

Other:

#	Response
1.	get picture of male partner form facebook
2.	we have not as of yet used only our web site
3.	We don't
4.	Connect with community members

21. How does your VAW program staff your social media presence?

Response	Chart	Percentage
Have a dedicated person to manage your social media		26%
Have a communications person whose job includes managing your social media		25%
Have one or more staff who share the job of updating your social media presence		42%
Other (please specify):		21%

Other:

#	Response
1.	
2.	pay honorarium, no one here has time
3.	Have hired someone to create a website
4.	outside resource

5.	We don't
6.	website is old, was put up years ago, not sure who maintains it but it's not all that in depth or useful
7.	Responsibility of ED
8.	self
9.	one staff as a side job
10.	usually me although I have farmed out to term staff a few times
11.	volunteer

22. Are any of these technologies used in office or offsite to communicate with or about the women, youth and children who are VAW program's service recipients?

	Yes	No	Don't know
Corded phones	91%	6%	3%
Cordless phones	50%	44%	6%
Cell/Mobile phones	80%	17%	3%
Internet-based phones (VoIP, Voice over Internet Protocol, calls like Skype, Vonage, Google Voice, use the internet rather than a traditional phone line)	18%	78%	5%
Text messages	57%	39%	4%
Pagers	3%	95%	3%
Caller ID (to screen, identify or sometimes block callers)	70%	30%	0%
Fax Machines	92%	6%	2%
Electronic Faxes (faxes received via email)	49%	44%	7%
Email	88%	12%	0%
Instant Messaging (online chats such as AIM, Google Chat)	5%	92%	3%
Relay Services (3rd party operator relays communications between the technology used by your worker and the offsite person who is Deaf, hard of hearing or has speech disabilities)	22%	68%	10%

Video Remote Interpreter Services (uses a web cam or video phone to connect the survivor/client and worker to an offsite sign language translator)	2%	92%	5%
Video Communication Software (such as iLink, GoToMeeting, Skype so survivors/service recipients can communicate with attorneys, friends, family, etc.)	8%	82%	10%

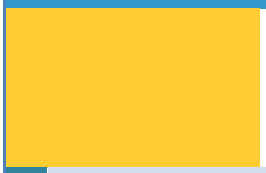
Section 3: Policies & Practices

These questions will help us understand the types of policies, practices, and procedures your agency has around using these technologies. The policies can be formal (agency policy manual) or informal (general understanding of proper protocol around using a particular technology).

23. What technology security and maintenance practices do you have to manage your VAW program's technologies?

	Yes	No	Don't know
anti-virus/anti-spyware protection installed on your individual office computers	97%	0%	3%
anti-virus/anti-spyware protection installed on your VAW program /agency server	67%	24%	9%
a dedicated Information Technology (IT) staff person or IT company/consultant who manages your VAW program's IT needs	53%	38%	8%
If your office has wireless Internet, is it protected with a password?	86%	5%	9%
If your office has wireless Internet, have you taken other security steps such as enabling strong encryption or limiting access to known computers/devices (by MAC address)?	24%	36%	40%
Does your agency provide a unique user name and password to each person who must access your agency's computers or networked server?	63%	32%	6%

24. If you have databases that store confidential, private and identifying information about people, does your organization do any of the following practices?

Response	Chart	Percentage
Password protect the database.		88%
Provide a unique user name and password to each VAW program worker who has access to use the database.		76%
Limit access to databases based on job roles. This may include limiting access to certain fields and client records.		73%
Ensure that third party IT consultants do not view the records in the database when fixing problems, doing routine maintenance or upgrades.		59%
Other		10%

25. Does your VAW program/organization have policies and practices that address safety, privacy, confidentiality and security for the following technologies?

	Yes	Being developed	Don't know
Social media: regarding work-related social media use	40%	40%	21%
Social media: regarding personal (non-work-related) social media use	40%	38%	22%
Recording or retaining photo or video images (whether for evidence collection or security/surveillance)	42%	35%	23%
Staff/worker use of personally owned technology onsite or offsite for the VAW program's work	38%	31%	31%
Participants use of personally owned technology devices and services (laptops, cell phones, tablets, cameras, location sharing or mapping) onsite	41%	28%	31%
Participants use of technology the VAW program owns and makes	47%	26%	28%

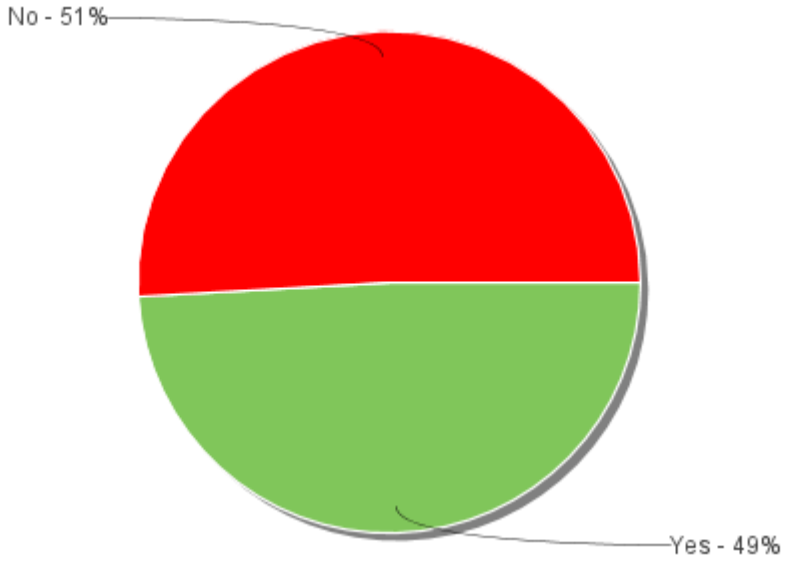
available: desktop computers, mobile phones, video games, etc.			
Providing Internet access for participants	52%	26%	21%
Use of location mapping, tracking, sharing or tagging devices and services in all aspects of your work	23%	43%	34%
Using Virtual Private Networks (VPN's) to access files remotely	24%	39%	37%

26. Does your VAW program have policies and practices that address safety, privacy, confidentiality and security for using technology when communicating with or about the women, youth and children and others who contact you or receive services and support?

	Yes	N/A	Being developed	Don't know
Land-line Corded and Cordless phones	65%	12%	14%	11%
Mobile/cell phones	63%	15%	15%	8%
Fax machines and e-faxes	70%	14%	8%	8%
Text messages	32%	45%	13%	12%
Pagers	7%	77%	5%	12%
Pay as you go phones	14%	70%	5%	11%
Location mapping, tracking, sharing or tagging tools	17%	51%	17%	17%
Email	62%	19%	12%	8%
Instant Messaging	13%	57%	13%	19%
Web cams or Video phones	18%	58%	11%	15%
Social Media	32%	37%	18%	15%
Relay services	9%	69%	9%	15%
Remote Video Interpreter services	4%	79%	8%	12%
Online Counseling or Service Provision	18%	60%	9%	14%
Technology personally owned	26%	42%	15%	17%

by staff			
16%	53%	16%	21%

27. If your organization is a provincial, territorial, Aboriginal or national association that has a primary purpose of representing and supporting local community-based VAW programs, are you working with your membership to develop policy and practice standards for VAW programs?



28. Which organizational technology policy and practice standards would your VAW program most like to see developed to address and protect safety, confidentiality, privacy, personal identity and security of workers, women and children.

Response	Chart	Percentage
Social media and networking		75%
Electronic communication (email, instant messages, texts, phones, VoIP, webcams, video conferencing, skype, etc.)		70%
Data and databases		57%
Technology use in counseling and service provision (email, real time instant messaging, live video, group chat rooms, video conferencing, Internet-based phone		57%

calls, etc.)	
Evidence Collection	38%
Mobile phones and other devices	58%
Location tracking, mapping, sharing and tagging devices and services	53%
Technology safety and privacy planning	60%
Identity protection planning	50%
Other (please specify):	8%

Other:

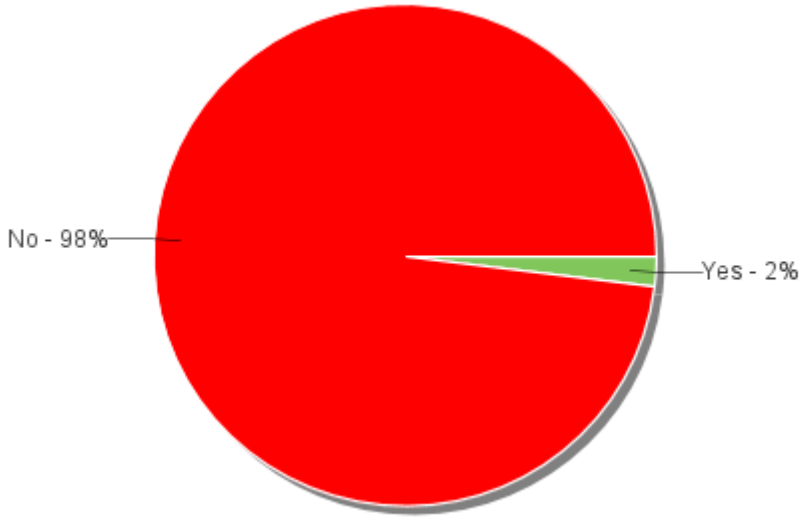
#	Response
1.	
2.	
3.	This is ongoing as tech. changes
4.	very uncertain what is needed
5.	education programs for clients so they are aware of technology use can put them at risk.

29. What barriers does your VAW program face in developing technology policies and practices that address safety, confidentiality, privacy, personal identity and security issues?

Response	Chart	Percentage
Lack of staff		49%
Lack of funding		68%
Lack of time		67%
How quickly technology changes and new technology appears		57%
How often technology companies (like Google, Facebook, Twitter) change their privacy policies		29%
Lack of knowledge or training on technology or on security steps		62%
Lack of knowledge or training on privacy and confidentiality laws and regulations		48%
Need more examples, samples or		61%

adaptable templates of technology policies and practices for VAW programs	

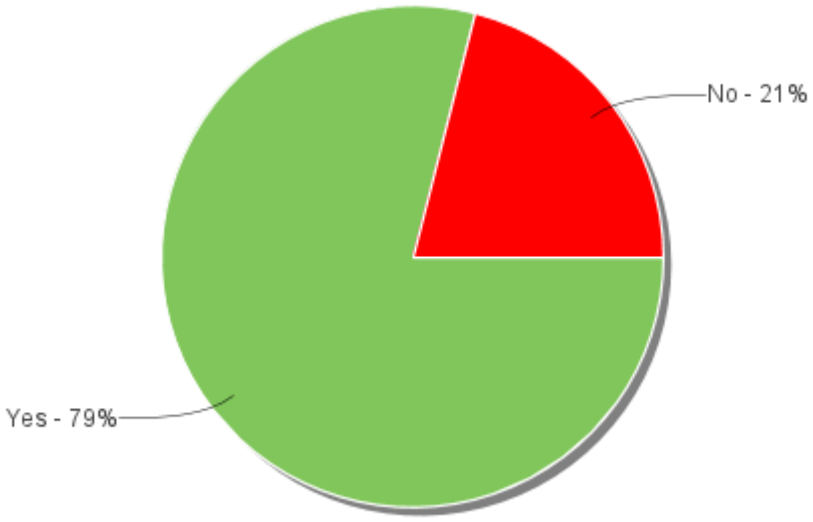
30. Do you have technology practices or policies you are using that you really like and would be willing to share as examples for other VAW programs?



31. Is there anything else you would like to share with us in this survey?

There were 7 responses to this question.

32. Would you like more information in the future when we have webinars and resource materials available?



If yes, please provide the email address(es) you want us to send announcements about future trainings and resources:

There were 52 responses to this question.

We thank you in advance and acknowledge NNEDV Safety Net for letting us adapt their survey. Your answers will help inform the work of Safety Net Canada.

APPENDIX B

Summary Report: Survey of Anti-Violence Workers on Technology Abuse

1. Canadian Province/Territory where you work:

Response	Chart	Percentage
Ontario		11%
Quebec		14%
Nova Scotia		3%
New Brunswick		1%
Manitoba		16%
British Columbia		36%
Prince Edward Island		2%
Alberta		11%
Newfoundland and Labrador		6%
Yukon		2%

2. Type of Program

Response	Chart	Percentage
Domestic/Family Violence		55%
Sexual Assault		5%
Both Domestic/Family Violence and Sexual Assault		38%
Other, please specify...		8%
	Total Responses	

3. What is your role in the anti-violence agency or program?

Response	Chart	Percentage

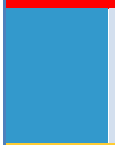
Executive Director/Program Manager		43%
Frontline Worker (support women, adult survivors)		40%
Children's Support Worker (support children and youth)		17%
Administrative Staff		3%
Information Technology Staff		0%
Community Educator / Trainer		6%
Volunteer		1%
Other		8%
	Total Responses	

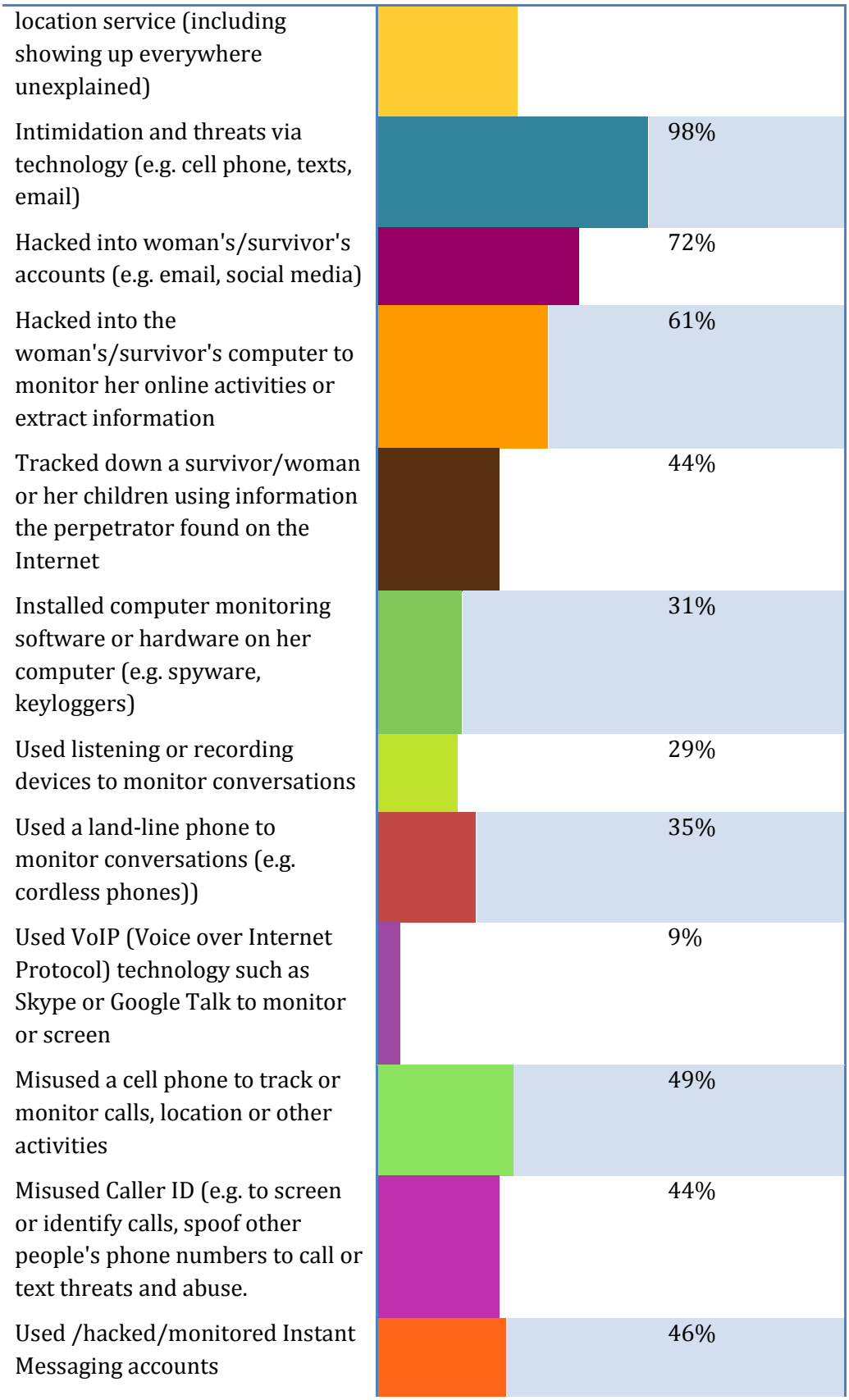
4. How many paid staff work in your anti-violence program?

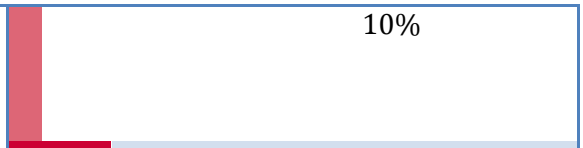
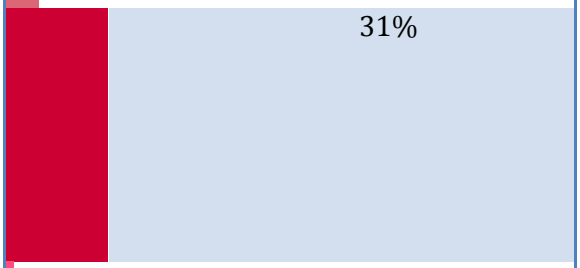
The average number of paid staff is 18.

5. Email Contact Information

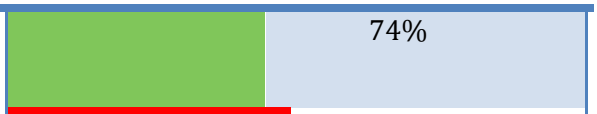
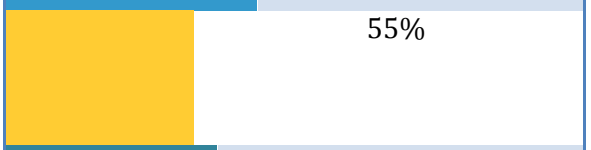
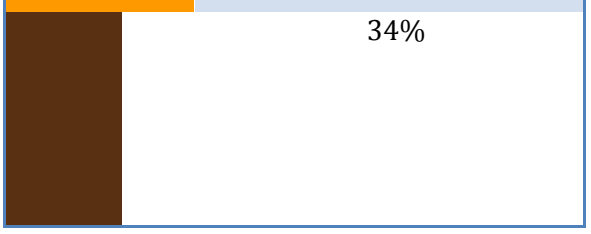
6. What have women and other survivors told you about the ways that perpetrators have (or are believed to have) misused technology?

Response	Chart	Percentage
Impersonation (using email, online profiles or other technologies to pretend to be the survivor or someone the survivor knows such as a friend)		69%
Distributed or posted pictures online of the woman/survivor without her consent		60%
Distributed or posted videos online of the woman/survivor without her consent		31%
Tracked the survivor's/woman's location via a GPS device or other		50%


location service (including showing up everywhere unexplained)
Intimidation and threats via technology (e.g. cell phone, texts, email)
98%
Hacked into woman's/survivor's accounts (e.g. email, social media)
72%
Hacked into the woman's/survivor's computer to monitor her online activities or extract information
61%
Tracked down a survivor/woman or her children using information the perpetrator found on the Internet
44%
Installed computer monitoring software or hardware on her computer (e.g. spyware, keyloggers)
31%
Used listening or recording devices to monitor conversations
29%
Used a land-line phone to monitor conversations (e.g. cordless phones))
35%
Used VoIP (Voice over Internet Protocol) technology such as Skype or Google Talk to monitor or screen
9%
Misused a cell phone to track or monitor calls, location or other activities
49%
Misused Caller ID (e.g. to screen or identify calls, spoof other people's phone numbers to call or text threats and abuse.
44%
Used /hacked/monitored Instant Messaging accounts
46%

Tampered with or destroyed assistive technology (e.g. hearing aid, screen reader, TTY machine)		10%
Used hidden cameras or her laptop's webcam to secretly watch or record the woman/youth/survivor without consent (e.g. undressing, having sex)		31%
Other, please specify...		3%
	Total Responses	

7. What kinds of assistance are women/survivors requesting around their own technology use?

Response	Chart	Percentage
Safety and privacy with social media (e.g. Facebook, Twitter)		74%
Safety with cell phones (e.g. talking, texting)		82%
Safety online (e.g. email, web browsing, instant messages)		73%
Safety with location privacy (e.g. tracking cell phones, geo-tagging)		55%
Safety with computer use		61%
Safety and privacy with cameras, photos, videos (e.g. tags, removal, face recognition)		40%
Safety and privacy planning around technology use		55%
Safety and accessibility with technology (e.g. assistive devices and services, website, hotline and shelter accessibility, relay services)		34%

Other, please specify...		3%
Total Responses		

8. What are some privacy and confidentiality concerns you have about using technology when working with or communicating with women/survivors?

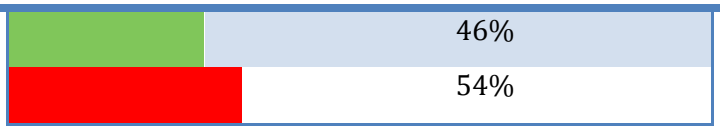
Response	Chart	Percentage
Perpetrators might intercept the communication		82%
Someone else might intercept the communication		60%
Support that is not face-to-face (e.g. lacks visual or verbal cues) might be misinterpreted or unclear		69%
Electronic communication might implicate our agency in ways that impact confidentiality (e.g. through a court order or a court case)		59%
How we communicate or maintain information might negatively affect the privacy and safety of a woman/survivor and her children		62%
Our agency has a confidential location that could be compromised		50%
Other, please specify...		5%

9. Do you feel you need more information and resources to best respond to requests from women/survivors about technology?

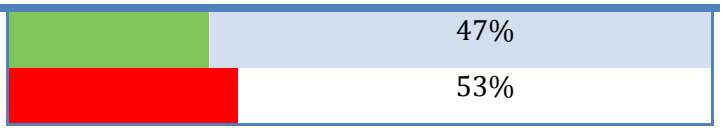
Response	Chart	Percentage
Yes		89%

No		11%

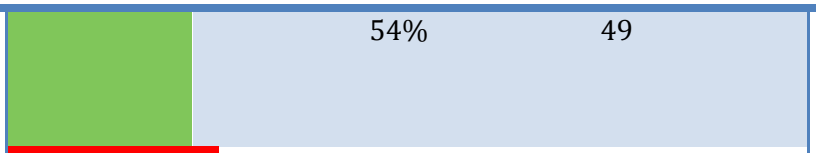
10. Are you aware of any complaints in your area involving technology-facilitated abuse where a law enforcement response was requested?

Response	Chart	Percentage
Yes		46%
No		54%

11. Was law enforcement in your community responsive to those complaints about abuse perpetrators misusing technology to harm?

Response	Chart	Percentage
Yes		47%
No		53%

12. If you think law enforcement is not responsive or prepared to address technology abuse, what do you think is the reason?

Response	Chart	Percentage	Count
Lack of awareness or understanding of technology and perpetrator misuse		54%	49
Lack of resources to investigate technology-related cases and crimes		60%	55
Minimization of cases associated with violence against women		62%	56
Lack of training about timely evidence collection regarding possible charges		40%	36
I don't know		21%	19
Others, please specify ...		9%	8
	Total Responses		91

13. Would you like more resources to help you work with law enforcement on issues related to technology abuse?

Response	Chart	Percentage
Yes		95%
No		5%

14. What are some ways technology is being used against women/survivors in court cases?

64 responses to this question.

15. What are some ways women/survivors have used technology to support their cases?

84 responses to this question.

16. What are some examples that you've seen in your community of technology evidence not being used or allowed by judges?

58 responses to this question.

17. Are you seeing judges mandate technology use between perpetrators and survivors/women?

Response	Chart	Percentage
Yes		40%
No		60%

18. Have women or other survivors been able to get civil legal recourse when a perpetrator has abused them through technology?

Response	Chart	Percentage	Count
Yes		8%	8
No		26%	27
I don't know		70%	73

19. Have you or your program worked with women/survivors who have had technology included in their protection or restraining orders?

Response	Chart	Percentage
Yes		54%
No		46%

20. What are some ways technology has been used against women, children or other survivors in family law cases?

50 responses to this question.

21. What are some ways technology has benefited women/survivors in family law cases?

51 responses to this question.

22. Would you like more information about legal protections and issues around technology and abuse?

Response	Chart	Percentage
Yes		97%
No		3%

23. If your anti-violence agency/program is involved in any community response teams or task forces, how are you using technology?

Response	Chart	Percentage
Our agency/program is part of a community task force or coordinated community response team		29%
Our agency/program and another agency currently shares the use of some		13%

technology (e.g. we use the same fax, wireless network, TTY machine, database , or, network server, etc.)	
Our agency/program does not currently share the use of any technology with another agency	59%
We have discussed how technology use in a community partnership impacts the safety, privacy and confidentiality of survivors/women.	39%
We would like more information on policies and practices to protect confidentiality, safety and privacy when using or sharing technology in community partnerships with other agencies	68%

24. Do you safety plan with women and other survivors around their own technology use and how the perpetrator might misuse technology?

Response	Chart	Percentage	Count
Yes		84%	88
No		16%	17

If yes, what types of technology do you most often safety plan about? What are recent technology issues that women/survivors have been concerned about?

77 responses to this question.

25. Do you have concerns regarding privacy and confidentiality when using technology?

Response	Chart	Percentage
Yes		76%
No		24%
	Total Responses	

26. What are other examples of technology misuse, concerns, issues that you would like to share with us?

33 responses to this question.

27. What are some innovative ways that women/survivors are using technology?

42 responses to this question.

28. This is the end of the survey. Thank you for sharing your insights. Is there anything else you want to share?

24 responses to this question.

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

Safety Net Canada 2013

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*, *Laurie Parsons*, *Rhiannon Wong*, *National Network to End Domestic Violence Safety Net Project*

French Translation: *Jose Beaudet*

Graphic Design: *Hannah Lee*

FINANCIAL

We thank the Office of the Privacy Commissioner of Canada for their financial contributions to this work and project.

Office of the Privacy Commissioner of Canada / Commissariat à la protection de la vie privée du Canada

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

SAFETY NET

cippic

NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE

TABLE OF CONTENTS

1. Introduction 4
2. What Problem Does A Database Solve? 5
3. Risks For Women, Youth And Children 6
4. Other Things To Consider When Using A Database 7
5. What Is A Database? 8
6. What Is Biometric Data Collection? 9
7. Data Collection Security 10
8. Different Ways Of Using A Data Base 12
9. Data Collection In Accordance To Personal Information Protection Act 13
10. Database Benefits For Programs 15
11. Database Risks For Programs 16
12. Database Vendor/Developer Considerations 17
13. Recommendations 18
14. Resources 19

1. Introduction

The electronic collection of data has been an emerging topic for discussion amongst violence against women (VAW) agencies/programs across Canada. As agencies move towards standardization through such processes as accreditation, it is clear that databases have been suggested as a tool to ensure that the quantity and quality of women, youth and children's personal information and, in some cases, case notes, are uniform.

There is also increased discussion about using biometric data collection (collecting finger prints and facial features for recognition) to keep women and anti-violence workers safe. Though this is a "state of the art" security feature, we encourage programs thinking about this option to read this document first in order to make women and child centered choices for your programs.

We would like to ensure that all agencies who serve women surviving family and domestic violence, sexual and dating violence, stalking, harassment, and abuse and their children are informed about the risks and benefits of various methods of data collection. We hope that this guide will help agencies to consider their options and weigh the risks and benefits so that they can make informed decisions that not only work for their programs but ensure that the safety, privacy and confidentiality of women, youth and children are protected.

Finally, this guide should be used in conjunction with many resources:

- Assessing Technology in the Context of Violence Against Women & Children. Examining Benefits & Risks. (Safety Net Canada)
- Canadian Legal Remedies for Technology-Enabled Violence Against Women. (Safety Net Canada)
- Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children. (Safety Net Canada)
- Records Management Guidelines: Protecting Privacy for Survivors of Violence www.bcsth.ca/content/general
- Privacy Toolkit www.bchousing.org/Partners/H_S_Op/Privacy_tools
- Non Profit Records Management Toolkit www.bchousing.org/Partners/H_S_Op/Administration/Records_management
- Provincial and territorial privacy laws
- Freedom of Information and Protection of Privacy Act
- Provincial and Territorial Child Protection Legislation
- Criminal Code of Canada

2. What Problem Does A Database Solve?

For many organizations, the appeal of a database is the apparent ease through which outcomes can be tracked and measured and used to demonstrate program "effectiveness" and/or to identify areas for program improvement. For other organizations, it is a way through which staff activity can be statistically monitored from a distance.

When considering purchasing or developing a database for the storage of resident/participant information, it is helpful to clearly identify the problem your agency is trying to solve within your programs.

- Are you having difficulty locating information that you need?
- Is there an alternative way to find it?
- Is it information that will always be useful to track or is your need for the information temporary?

If the benefits of databases were self-evident, they would sell themselves. Remember that database companies must establish a need to create a demand for them to fill. Consider the following questions before deciding if your agency/program needs a database:

- How will a database help you to fulfill your organization's mission statement?
- Is it congruent with your organization's values?
- Could it result in staff/volunteers working more with computers and less with residents/participants?
- Will it require staff to ask questions of residents/participants that may influence either negatively or positively the nature of their relationship?
- Will it cause staff to sit across a desk from residents/participants as they type information into a computer?
- Are you able to ensure the security, privacy and confidentiality of the data collected?

Some database companies provide for the sharing of information between agencies. Remember that sharing information about residents and/or former residents and participants could be in direct violation of your contract with most funders without the explicit request from and/or informed consent of a resident/participant.

When considering databases, think about:

- Upholding a participant/ resident's right to privacy and the ethical implications databases may possess.
- Women's safety and security and the implications databases may have on safety.
- Do databases help eliminate violence? At times can databases help abusers/stalkers perpetuate violence further?
- What is the direct benefit of databases for the women and children you serve?

3. Risks for Women, Youth and Children

When considering the liability that databases can cause agencies, it is critical to think and consider the implications that databases have on the safety of women youth and children. Here are questions to consider:

- What happens if Citizen and Immigration Canada subpoenas or provides a court order for your data and finds women without immigrant, refugee, and/or Canadian citizenship status accessing your program?
- What if the data you collect is run against a police database and the survivor has charges against her? What would this mean in terms of protecting the confidentiality and privacy of women?
- Some databases ask programs to collect unnecessary information about a woman, youth or child. The collection of irrelevant information into a database, such as information about women's abusers, can put women at risk for legal complications such as libel and 'Defamation of Character. '
- The collection of Biometrics does not allow the flexibility to protect a woman's confidentiality. If your agency has a security system that requires a resident to provide her finger prints in order to access transition housing/shelter, there will always be a record that she accessed services at your program on a specific date.
- Does an agency's decision to use and store biometric data as a form of safety outweigh the possibility of putting women, youth and children at risk of 'unintended consequences?' See biometrics page 9.
- What are the risks for women's safety if a woman's ex-partner or an associate of her ex-partner works for the database company that is hosting her data?
- Consider the significant privacy and civil liberty implications of collecting too much data such as social media accounts, pictures of residents/participants and their children, Social Insurance Numbers and immigration statuses.
- How vulnerable is your database to theft, hacking or abuse? Is it located on a computer connected to the internet?
- If a resident/participant file is subpoenaed, how will you ensure that all other records on the database are not compromised?
- What are the implications of having an electronic trail of your service that essentially can never be completely deleted?

4. Other Things to Consider When Using a Database [1]

Necessity
What problem is your agency trying to solve? Is a database really the answer? For example, a community experiencing difficulties with protection orders being served may want to create a database thinking that it will make the process more efficient. Creating a database doesn't address the problem of orders not being served because the problem is not having enough officers to serve the orders.

Functionality
Is the database you choose user friendly? Has your agency allocated sufficient money, resources, and staffing to keep the database up to date and make it useful? Has the agency allocated funding and staff time to conduct annual privacy assessments? Has the agency allocated sufficient resources for training existing and new staff (turnover) and providing ongoing technical support?

Privacy & Safety
What confidentiality and privilege laws/regulations/obligations apply? Who will have ultimate responsibility for ensuring that confidential data is protected? Is there a designated privacy officer within the organization? Do users sign documents acknowledging their responsibilities for protecting the confidentiality of data, such as a data confidentiality agreement or an employment agreement with data confidentiality provisions? Are these incorporated into agency policy?

Resident/Service Recipient Information
What factors will agencies use in establishing collection, modification, use, and disclosure procedures for identifiable data? Are women and children informed about the security and data sharing policy? What is the process for residents/participants to opt-out, inspect, withdraw, or correct their data/records? How will agencies inform women and children about this process? How will they ensure that the data is completely gone if a woman/child opts-out of having her personal information collected in a database?

Cost
Has the agency priced multiple options and received at least 2 bids for the project? Has the agency done a cost benefit analysis to assess the balance between ongoing costs and ultimate benefits? Has the agency designated appropriate funds for the project? While modest expenses for outcomes measurements are part of any grant, a direct services grant should primarily fund services and not outcomes measurement.

Security
Best practice is to secure backups at the same level of security as the original source. Has the agency included plans for system backup and security? How will they ensure all data is encrypted? Consider contracting with a computer security professional to assess the penetrability/security of the system and to recommend improvements.

[1] National Network to End Domestic Violence, Safety Net Project, "Databases." Washington DC, 2008

5. What is a Database?

Databases are computer programs used to organize information in a way that can make information easy to locate, access, and update. Databases can be organized in a variety of ways (alphabetically, numerically) and can include text, words, and images. Databases can be searched using a "query" like a name, place, date, etc to find information about groups of people. Databases have a "report" function which allows the user to run reports on such things as the number of new residents/participants in the last month or the most popular resource accessed, etc.

Databases generally allow 'administrators' (it is best practice to have one person in your office responsible for the database such as the Executive Director, program manager, IT staff or member of your administration team) to set usernames, passwords, access levels, and permissions. Additionally, well-designed databases incorporate audit trails to provide a detailed record of the queries and actions of each user. Databases can be designed at the outset to automatically purge or delete certain data elements after a certain time period and only retain the elements necessary for reporting purposes.

- **Access levels**
  Access levels enable an administrator to who can access database information and to set a variety of access levels. For example, the system administrator could establish access levels so that a few staff to see all the information in a database, and other users to only see the information relevant to the role of the user (volunteer, staff, attorney, etc.). Before the database is put into place, it is important to determine who needs to access the data, what level of access is appropriate, and how access to the data will be limited to these authorized persons.

- **Data storage**
  Some databases are hosted locally while others are hosted off-site. A locally hosted database means that the data remains in the agency, on the agency's server. A remotely hosted database is often a commercial package, whereby the agency pays a monthly fee and the database is hosted by a third-party, outside the agency. For more information see Section 4.

Pre-packaged, commercial databases are often less expensive up front, but may not be adaptable or may require additional costs to modify the database or create a new type of report, etc. If agencies choose to contract with someone to have a database developed especially for the agency, a limited number of modifications can be written into the initial contract. The costs to develop, implement, and maintain a database can range widely from $5,000 to over $50,000.[2]

[2] National Network to End Domestic Violence, Safety Net Project, "Databases." Washington DC, 2008

6. What is Biometric Data Collection?

Biometric data collection aims to automate personal identifiers such as eye colour, finger prints and face shape by comparing "information scanned in real time against an "authentic" sample stored digitally in a database"[3]. For example, Jane will be staying at your transition house/shelter for 30 days. At intake, the intake worker 'scans' Jane's finger print into your agency's security system. The security program is set to allow Jane to leave and return to the house after Jane scans her finger every time she wants to leave or return (in real time) and the security program recognizes her finger print as a match (authentic sample) in the system.

VAW programs have access to this option when purchasing "high tech" security systems. Options to store a woman, youth or child's finger prints and facial features has become a featured selling tool for those programs in need of high security and is often promoted to better control access to physical facilities such as housing programs.

Since 9/11, biometric security systems have increased in popularity and aim to identify individuals and track movement. The cost of these systems has decreased significantly and can be included in a comprehensive security program for approximately $10,000.00.

Each VAW program must consider the unintended consequences of collecting biometric data in addition to the database considerations listed in sections 2 and 3. Agencies have to work through the questions below before making an informed decision that puts women's privacy and safety first.

There are major risks to consider when choosing biometric databases.

- Have you ensured that biometric data cannot be intercepted or stolen?
- Is all data, especially biometric data encrypted? How have you ensured that all encrypted data cannot be "unencrypted"?
- Do all users have strong passwords?
- Because biometric data is personal and interception, hacking and loss of biometric data can have detrimental consequences to women and children, how have you ensured that biometric data is deleted permanently once a resident/participant has left your program? Is this possible?
- Do you have informed consent from residents/participants to collect and store their biometric data? How have you ensured that they understand the unintended consequences of providing your program with biometric data?
- What happens if a survivor does not consent to storing her biometric data?
- Is your agency prepared for any legal implications that could happen if data, privacy and confidentiality are breeched?
- Has your agency allocated funding to conduct regular privacy assessments, ensure encryption is up to date and have an IT consultant/staff available for any immediate concerns?

[3] Electronic Privacy Information Center, "Biometric Identifiers." http://epic.org/privacy/biometrics/#bg Retrieved November 10, 2011.

7. Data Collection Security

A) Data Storage Options

Data security, confidentiality and privacy breech polices need to be in place before utilizing electronic databases as a data breech can be life threatening for women, youth and children who have fled/or living with the effects of domestic and family violence, sexual and dating violence, stalking, harassment, and abuse. Data breeches can also be financially costly to an agency.

Personal information can be stored in a database in two ways:

- Remotely through the Internet.
- Locally in your agency on your agency's server.

There are safety implications for both.

i) Database platforms that require internet access have a variety of security risks that need to be considered.
   - One must consider the risk of 3rd parties (commonly known as hackers) potentially accessing participant information through the internet. Ensuring that all files are encrypted is one safety measure however, not if the 3rd party has access to an agency staff's user name and password.
   - If staff have access to the database outside of their workplace, it is important to consider the possibility of user name and passwords being stored on public and personal computers, compromised by other people accessing the computer or simply a 3rd party viewing a staff member enter in their user name and passwords over one's shoulder.
   - There is always a possibility that computers get misplaced or stolen. Are user names and passwords stored on these computers?
   - Database companies often have access to an agency's database in order to solve any "glitches" or make any changes required. This access compromises the confidentiality of residents/participants as database companies can access your database at any time without restrictions.

ii) Databases that are hosted on an agency's server and do not require internet access also have security concerns.

   Here are some considerations when considering server based databases:
   - If your agency server is connected to the internet, 3rd parties (commonly known as hackers) are still able to access your database.
   - Consider who has access to the space where your agency's server is stored? Do volunteers, staff, outside janitorial staff, utility companies, participants/residents or other service providers have access to the space where the server is stored? Can someone walk into your space and pick up your server and walk out with it?
   - If the database company is hosting your database on their own server, essentially they have access to the files your agency uploads to the server.

- If your database is stored on your own server, consider how the database company has access to your database for maintenance purposes.

Note: databases can be used to store non-personal information, in fact if you are going to use a database, try to design it as best you can to collect information about requested and provided services versus personally identifying information.

B) Security for Paper Files

Paper files also pose a security risk when storing personally identifying information.

Programs should:

- Ensure that filing cabinets or safe to store paper copies of participant/ resident records and removable hard drives are in locked filing cabinets. With this, agencies should have plans in place if the filing cabinet key is lost or stolen.
- Filing cabinets should be in locked rooms with limited access.
- Clearly defined access levels should identify who has access to the keys for the filing cabinets, storage rooms, and offices. Access should be defined based on the person's job role and a "need-to-know" basis.[4]
- Consider who has access to the paper files and filing cabinets. Volunteers, staff, outside janitorial staff, utility companies, service recipients or other service providers accessing your space? Can someone walk into your space and wheel out your filing cabinet?

For more information see "Records Management Guidelines"
www.bcsth.ca/sites/default/files/Records%20Management%20Guidelines%20April%202006.pdf

[4] Field, Julie. Securing Paper and Electronic Information for Co-Located Sexual Assault/Domestic Violence Programs and Partners. Washington DC, 2008

8. Different Ways of Using a Data Base

There are many ways of utilizing a database. It is important that an agency considers its needs before purchasing one.

Personal Information Database
Some agencies prefer a database to collect personal information only. This type of database is usually one that is hosted on an agency's server and can be developed easily on applications such as Microsoft Access. These databases collect basic personal information such as participant name and contact information.
Another option for personal information only databases is to use the database as "more of a "card catalog" to reference paper files. Here the data is entered with a non–identifying code instead of a name. Paper files are labeled with the same code and this helps staff know which filing cabinet to go to in order to find the paper file."[5]

If connected to the internet, these databases are at risk of being compromised by 3rd party hackers not to mention subpoenas/court orders and other persons who may have access to the database.

Case Management Database
Some agencies use participant/ resident databases as the primary means of information storage. This might include inputting personal information and extensive details such as which programs were accessed, background information such as abuser information and child information, programs accessed, case notes and referrals. Often the collection of funder required statistics are inputted in this database for easy data collation for monthly and quarterly reporting.

The reality is the risks of breaching confidentiality and privacy is high. Personal details inputted into databases put the lives of women and children at risk. See page 16 for the risks associated with databases.

Biometrics Storage
Some agencies consider using biometric methods. These will be marketed as ways of ensuring building security. However, using biometric methods to enter a program/shelter does not ensure the safety of the women, youth, children and staff.

When using biometrics it is important to consider where biometric data is being stored and how. Is it encrypted? How can a perpetrator hack into the biometric database and steal personal information? What happens when biometric data is deleted? Also consider what happens if there are false positives (allowing access to an unauthorized service recipient/staff) and false negatives (denying access because the program has misread a finger print) when the computer program is comparing biometric information. One must also consider the safety risks to women, youth, children and staff may be irreversible. For example, in 2005, car thieves in Malaysia cut off a finger of the owner of a Mercedes Benz in order to get around the owner's high tech security system.[6]

[5] National Network to End Domestic Violence, Safety Net Project, "Databases." Washington DC, 2008
[6] Kent, Jonathan "Malaysia car thieves steal finger". http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm BBC Online (Kuala Lumpur). 2005. Retrieved 15 November 2011.

9. Data Collection in accordance to BC's Personal Information Protection Act: An Example

From the example listed in section 5, we know that collecting too much data on an electronic database can increase danger and risks for women, youth and children. It is suggested that agencies choosing to use an electronic database follow privacy legislation such as BC's Personal Information Protection Act (PIPA). Though this is a BC specific example, provincial and territorial privacy legislation can be incorporated into this table.

Below is a table that outlines the legal privacy requirements for BC organizations collecting personal information on databases and what to consider before inputting service recipient's personal information on to one.

According to PIPA Agencies:	Database Implications to Consider
Must receive consent in order to collect, use and/or disclose personal information. [7]	Informed consent is best practice. Let the participant/resident know that their personal information will be uploaded to a database and who has access to this database (IT, Developer, Staff members/volunteers) and the risks associated with this.
Must not, as a condition of supplying a…service, require an individual to consent to the collection.[8]	Have plans in place for when a participant/resident decides they do not want to have her personal information collected. If you are using your database to input statistics, how do you do so? Are paper files an option for back up?
On request of an individual, an organization must provide the individual with the following: • the individual's personal information under the control of the organization; • information about the ways in which the personal information ...has been and is being used by the organization; • the names of the individuals and organizations to whom the personal	• Is your database capable of printing off the participant/resident information/electronic case file without jeopardizing other women's information? • Have information about how your organization is using personal information in the database ready. • Remember to include the database developer and their staff if they have access to your database.

[7] Office of the Information and Privacy Commissioner. "Personal Information Protection Act," http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm Retrieved 24 November 2011.
[8] Office of the Information and Privacy Commissioner. "Personal Information Protection Act," http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm Retrieved 24 November 2011.

information ...has been disclosed by the organization.[9]	
Must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.[10]	Are your database files encrypted? What happens when the encryption can be "decrypted" by 3rd parties (hackers)? Does your agency have firewalls and anti-virus software? What policies do you have in place for if 3rd parties do access your files or your agency server is physically removed? What access levels will staff have? What security plans do you have in place for backups or disposing of old hard drives?
Must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that: • the purpose for which that personal information was collected is no longer being served by retention of the personal information, and • retention is no longer necessary for legal or business purposes.[11]	A computer's data can almost always be recovered. Have a plan to physically destroy all computer hard drives that have access to the database when your agency decides to upgrade hardware. Have a plan in place for when to delete a resident/participant file after their file has been closed and the retention period for records is over. (Discuss with the developer if deleting a file permanently is possible if your agency is still utilizing the database).

For more information on BC's Personal Information and Privacy Act click here: www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm#part3

Other considerations:

- Data and privacy laws vary from province, territory and country. Know what laws apply to your data if your participant's files are stored in a jurisdiction other than your own. Ask who owns the records if they are being stored offsite?
- Have a plan in place for if your whole database gets subpoenaed/court ordered instead of the individual file sought in a court case or by law enforcement.

[9] Office of the Information and Privacy Commissioner. "Personal Information Protection Act," http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm Retrieved 24 November 2011.
[10] Office of the Information and Privacy Commissioner. "Personal Information Protection Act," http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm Retrieved 24 November 2011.
[11] Office of the Information and Privacy Commissioner. "Personal Information Protection Act," http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm Retrieved 24 November 2011.

10. Database Benefits for Programs

Agencies are likely to choose a database based on a variety of benefits.

- Databases allow agencies to easily analyze relationships between data and run reports on service usage.[12]
- Resource databases eliminate the need to recreate materials or resources and generally offer keyword searches to provide quick results.[13]
- Databases offer agencies the benefit of standardizing their method of data collection.
- Databases provide service providers with one system that is easily accessible to users.

[12] National Network to End Domestic Violence, Safety Net Project, "Databases." Washington DC, 2008
[13] National Network to End Domestic Violence, Safety Net Project, "Databases." Washington DC, 2008

11. Database Risks For Programs

Before purchasing a database, agencies must consider the safety risks in order to maintain the privacy and confidentiality of its participants/residents.

VAW Program Database Considerations

- Data kept on a computer that has Internet access is vulnerable to interception or breaches. A security breech can happen on many levels. Agencies need policies on who has access to the database, physical security of the agency's server, and security against 3rd party breeches such as "hacking."
- Agencies are often served with subpoenas and/or court orders for the records of participants/residents. Agencies need policies in place for this occurrence, including how not to put other participants/residents records at risk and how to let the participants/residents know that their records have been subpoenas or court ordered.
- Remember that any information entered into a database could exist for perpetuity. Even if the database owner promises to delete it after a certain number of days, data can be backed up, removed, exported, screen shot etc. It's important to carefully consider what is collected and what the future implications may be. This is important to consider after the woman leaves shelter. Does she own or have access to her data?
- Although it's highly unethical, there is always a risk that data collected for one purpose will be used for secondary purposes (such as intake information being used by researchers for research studies). Additionally, there is a risk that current or former employees will purposely or accidentally share confidential information or take advantage of their access to the database to perform searches for personal use.
- Untrained users may accidentally delete or alter data.
- Would you refuse service if a woman does not want her data stored in a database?

12. Database Vendor/Developer Considerations

- It is best practice to ensure that database vendor/developer employees DO NOT have access to your database. Often, database vendors will confirm that vendor employees do have access but that they have signed a confidentiality waiver. It is important to ask the vendor questions on what happens if a vendor employee breeches that confidentiality agreement.
- If a vendor hosts an agencies data, can a vendor deny agencies their data through the closing down of business, technical problems, etc?
- Agencies must clarify in a legal written contract who owns your agency's data once it is stored on the vendor's server or in a cloud database system.
- Does the vendor have policies on what happens if they get subpoenaed/provided a court order for your participant/resident record and will they let your agency know if they do?
- Ask the vendor what security measures are in place to protect your agency's data and services? For example, is the data encrypted and if so, who has the encryption key?
- If the provider goes out of business, what happens to your agency's data and services?
- Your agency is liable for the personal information uploaded into a database. Have legal contracts written to ensure that survivors' privacy, confidentiality and personal information is being upheld.

13. Recommendations for Database Privacy and Women's Safety

- If your agency is using a database, agency staff must obtain ***Written, Informed and Time Limited consent*** from participants/residents acknowledging that they know their information is being stored in an electronic database and are informed about the security and confidentiality risks associated with this method of data collection.
- Ensure all data is encrypted. Have plans in place for if data becomes "unencrypted."
- Individualize ***Levels of Access*** for each member of staff, volunteers who have access to the database. Do administrators, volunteers and management need access to all files if they are not working with women, youth and children directly?
- Have a plan in place if the main administrator of the database leaves, takes unexpected time off or is sick. Who knows how the database works?
- Have a plan in place with the database developer for if they are no longer in business or there is staff turnover. Who owns the files? What happens to women's information if it is hosted on the developer's server?
- Work with the Database Developer to plan for potential subpoenas/court orders for confidential files/records. Ensure is a legal written contract that the developer will let you know that files have been subpoenaed/court ordered and whose file it is. Is there a time frame they will contact you by? What is the policy around this? Note that your agency is liable for the developer's actions with personal information.
- Organizations should protect any personally identifiable information collected about a participant/resident since any data leaks or breaches could be fatal.
- For safety reasons, we recommend that organizations not store confidential or personally-identifiable information about participants/residents on any computer that is connected to the Internet. Without an internet connection, there is significantly less risk that an abuser/stalker will hack in and access your organization's data, or, that a virus will infect your computer and automatically emailing confidential files out to others.
- Collect information only necessary to do the job. Database sales representatives typically showcase database perks such as storing photos, Facebook account information, names and addresses of the abuser and immigration/refugee/First Nations/Metis/Inuit or Non Status information. Collecting unnecessary information can pose risks to women's safety. Work with the Database Developer prior to launching your database in order to ensure that only necessary fields in your database.
- Have plans in place for if there is a privacy complaint made against your agency. Consider what potential outcomes could be if data has been breached, hacked and the lives of women and children are put at risk.

14. Resources

- Organizational Technology Practices for Anti-Violence Programs. Protecting the Safety, Privacy & Confidentiality of Women, Youth & Children. (Safety Net Canada)
- www.nnedv.org/docs/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf
- www.nnedv.org/docs/SafetyNet/NNEDV_DataSecurity.pdf
- www.bcsth.ca/content/general
- www.bchousing.org/Partners/H_S_Op/Privacy_tools
- www.bchousing.org/Partners/H_S_Op/Administration/Records_management
- Provincial and territorial privacy laws
- Freedom of Information and Protection of Privacy Act
- Provincial and Territorial Child Protection Legislation
- Criminal Code of Canada

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

Safety Net Canada 2013

SAFETY NET

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
French Translation:	*Jose Beaudet*
Graphic Design:	*Hannah Lee*

FINANCIAL

We thank the Office of the Privacy Commissioner of Canada for their financial contributions to this work and project.

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

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
NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE

TABLE OF CONTENTS

1. INTRODUCTION 4
2. CAPACITY, READINESS, ETHICS AND LIABILITY 4
3. CREATING YOUR ONLINE PRESENCE 6
4. POSTINGS: DATA PRIVACY & PERSONALLY IDENTIFIABLE INFORMATION 7
5. CONSIDER YOUR AGENCY POLICY FOR SOCIAL MEDIA “FOLLOWERS”, “FRIENDS” AND CIRCLES 7
6. SOCIAL MEDIA & ACCESSIBILITY 7
7. STAYING CURRENT 8
8. SUPPORTING WOMEN, YOUTH AND CHILDREN 8
9. PERPETRATORS USE SOCIAL NETWORKS & MEDIA TO STALK AND HARASS 9
10. GIVING UP SOCIAL NETWORKS IS NOT THE ONLY OPTION 10

1. Introduction

Social media is used by violence against women programs (VAW) for many reasons. Anti-violence agencies organize events online to empower women and youth, support the voices of survivors, engage the community in preventing and ending violence, and honor the women and children who have died as a result of gender-based violence. These events and training announcements are distributed via email and posted on websites, Facebook and other social media pages with links to online registration forms or email addresses. VAW programs also organize online or mobile phone campaigns and events.

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. Many VAW programs also provide cross-sector, community-based and age-appropriate school-based violence prevention and skills building programs. VAW programs have created apps, videos, quizzes and games to empower women and girls. When engaging in public outreach via technology, it is important to assess the capacity of one's program and the potential impact on privacy, confidentiality and safety.

This short guide will assist programs to determine their capacity to use social media and examine the potential risks that social media has for VAW agencies, women, youth and children. This process will support VAW programs to develop promising practices and policies around social media use.

2. Capacity, Readiness, Ethics and Liability

Before deciding which social media platform to use, it is important for agencies to consider the following:

- Staffing Capacity:
  - Who will be the dedicated staff or volunteer to coordinate social media?
  - Will they have the capacity to monitor posts by the public 24/7?
  - Is staff prepared to be contacted by site visitors?
  - Will they have the capacity and equipment to post news and events on behalf of your agency?
  - Will that staff or volunteer need training?

- What are the costs?
  - Does the social media application have a cost?
  - What about the staff/volunteer time needed?
  - Are training costs involved?

- Communication plan:
  - Does your agency have a communication plan in place? This might include the type of messages, news articles or campaigns that your agency would like to support/promote.
  - Do the events, campaigns and news align with agency mission, values and ethics?
  - Can you provide a safety alert about using a safer computer/phone due to the risk of computer and mobile device monitoring such as through spyware?
  - Provide visitors with emergency numbers (with area code), agency contact information, and links to your website.

- Is your communication plan realistic?
  - 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 at a time.
  - How will you promote your online presence?

- What are your goals for engaging in social media?
  In our 2013 survey, "Organizational Best Practices," VAW programs across Canada said their social media goals were to:
  - Engage and mobilize the public.
  - Ignite social change.
  - Broaden social awareness.
  - Influence the digital discourse.
  - Challenge disparities in digital worlds.

- Who is your audience?
  - Different age and cultural groups use different social media/network applications. Discuss benefits of using various applications (for example Facebook, Twitter, My Space, Instagram) and who they will reach.

- Ethics and Liability:
  - How will you include clear contact information on your social media/network page?
  - Will your agency be able to respond to request from survivors timely?
  - Often survivors will inquire about support or share their story on a VAW programs social media/network page like Facebook. How will your agency protect the confidentiality of survivors?
  - How will you let them know that what they post on your social media/network application is not confidential and can have unintended consequences?
  - What if you are obligated to take action legally?
    - How far do you "investigate"?
    - What if you don't respond?
    - What if perpetrators post threats and harassing messages to staff and survivors on your social media/network page?
  - Be transparent and develop policies about social media and location privacy practices:
    - For devices personally owned by staff.
    - For devices owned by the agency.
    - For devices that survivors bring with them such as laptops and mobile phones.

It is the responsibility of the agency and staff to strip geotags from photos and videos posted online

3. Creating Your Online Presence

Here we outline practice considerations when creating your online presence:

- Staff and participant boundaries:
  - Are staff and (former) participants/residents able to connect with each other through personal social media/networks?
  - What are the potential risks?
  - How can programs develop policies that ensure privacy, safety and confidentiality of the women, youth and children they support?

- Be clear and transparent: On all of your social media platforms, provide notice about how public or private your social media platform is. Inform survivors that their computer could be monitored. Let survivors know that if they choose to contact your program through social networks, when they expect a response.

- Develop a policy about responding and removing posts.
  - What do you post?
  - Are others allowed to post on your site/page?
  - Consider what posts can stay, what needs addressing and what needs to be removed?
  - Are you filtering or monitoring the posts?
  - Remember, once a post is made, it is never truly gone.

- Discuss what role your agency has in reporting and collecting evidence. This may be necessary if perpetrators or members of the public threaten women and children accessing your program or agency staff.

- Will you have a private or public social media presence?
  - When considering who your target audience is, discuss options for private Wikis, blogs, Twitter accounts and closed social media groups. Not all social media is public.

- 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 conversation?

4. Postings: Data Privacy & Personally Identifiable Information

- Do not post personally identifying information (name, photos, and videos) about staff, colleagues, financial supporters or people who attend an event you host unless your agency has informed consent.
- Do not share survivors' personally identifying information.
- Do not share details about a survivor's case or situation.
- Do not solicit information about abuse or conduct counseling or advocacy using social networks.

5. Consider Your Agency Policy for Social Media "Followers", "Friends" and Circles

Each social media site works differently. Create a general policy and then develop practices for each site. Consider what policy to have if VAW program participants/residents send a "Friend" request to, for example the Facebook page of a VAW program staff member. Discuss general practice and anticipate case exceptions. As a default practice:

- Do not underestimate the interconnectedness of online spaces.
- Do not "friend" active VAW program participants/residents.
- Do not "friend" survivors without their permission.

Develop social media boundaries and practices for situations where a VAW program staff member is already a social network "friend" of someone who then accesses your VAW program's services.

Also develop policies about how will you address problematic posts.

6. Social Media & 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.

"While social media networks still present access barriers, there are steps organizations and individuals can take to reduce them"[1]

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

Social media keeps evolving and this impacts how accessible the social network agencies are using will be to different people with varying abilities. When VAW programs evaluate what social media tool to use they should review and consider:

- Which social media applications are currently accessible, to what extent, and do they have a reliable history of designing accessibility into each upgrade?
- 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?

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. This is because it is often the privacy and security settings that are updated and are automatically reset to the settings which are the least private and secure. VAW programs have to 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

Often women, youth and children will 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 victims on social media sites.
- Defense attorneys who try to get access to information about rape survivors from social media sites.

9. Perpetrators Use Social Networks & Media to Stalk and Harass

It is helpful to safety plan with survivors about their own social media use. Perpetrators use social media and networks as a form of technology-enabled abuse. Some examples of technology-enabled abuse through social media are:

- Create fake accounts of the victim or of a victim's friends or family members to impersonate and gain more information about the victim.
- Monitor victim's (and her children's) social media pages to determine their location and what schools or activities victims are participating in. They can also establish patterns through posts.
- Post nude or semi-nude photos and videos of the victim.
- Harass, coerce and/or threaten the victim through social media posts or private messages.
- Post harassing or inappropriate messages on victim's friend's pages as well as agency pages.
- Monitor her page and coerce her into updating certain things.
- "Friend" the victim's friends & 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 for privacy, security, blocking.
- Temporarily decreasing, changing or stopping postings.
- 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 others who might eventually see or share it?
- 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 a screen on a Smartphone or computer, printing a webpage as a PDF file and other options.
- How to opt in and opt out of various automatic location services.
- Refraining from revealing location through 'checking 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 part of a stalking or harassment charge.

10. Giving Up Social Networks is Not the Only Option

Social media and networks may be a helpful support system for survivors. 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 for women and youth fleeing technology-enabled abuse to consider:

- Who might respect your heightened need for online privacy & 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?