Cyberviolence Prevention Policy and Best Practices; Cost-Benefit Analysis

This document was prepared as a resource for the stakeholders of the Atwater Library and Computer Centre's Preventing Cyberviolence Project, as they adopt definitions and develop policy for their organizations.

Prepared by Shanly Dixon, PhD, Bianca Baldo, B.A., LL.L and LL.M and Lukas Labacher, C.Hyp., BA Hons (Psych), MA (Ed), PhD Candidate (Social Work/Social Policy) for the Atwater Library and Computer Centre's Project Cyber and Sexual Violence: Helping Communities Respond under the theme of Preventing and eliminating cyberviolence against young women and girls funded by Status of Women Canada (April, 2014-April, 2017)

Status of Women Canada | Condition féminine Canada

Executive Summary

The findings from our needs assessment, conducted in April, 2014, revealed a critical need for stakeholders to develop and adopt clear definitions and policies around cyberviolence. According to our stakeholders, the absence of clear definitions and policies makes it nearly impossible to prevent and address cyberviolence in their schools, workspaces and community organizations. Therefore, the first purpose of this cost-benefit analysis is to inform and empower our stakeholders regarding how to implement and apply definitions of cyberviolence, directed at girls and women, LGBTQQI2S and gender non-conforming people, that are directly applicable to their communities and organizations. The second purpose is to support and work directly with our stakeholders in drafting policies and practices that not only prevent cyberviolence in their organizations, but also respond to and support individuals who have been affected by it. Through a participatory process, we strongly advocate for strategies that combine legislative and policy solutions, which we believe will be most effective in actively addressing the gendered, racialized, and sexualized nature of online violence.

The goal of this strategy is to work directly with a variety of stakeholders, in education, academia, law enforcement, security, and health and counselling occupations, as well as in the video game and technology industries, so that we may assist them in developing and adopting clear definitions of cyberviolence, polices for prevention, steps to supportive services and resources for those who experience cyberviolence. To ensure the long-term benefit of such a strategy in a continuously evolving technology climate, we focus on the people and the organizations and communities in which they operate rather than the rapidly evolving technologies. We assist stakeholders in creating policies that work best for them, their individual context, and their unique organizational structures. In so doing, we aim to provide the tools necessary to draft a living *Cyberviolence Prevention Policy and Best Practices* that each organization can uniquely apply and frequently update to adapt to their evolving organization and technologies.

Due to the ever-increasing blurring of boundaries between people's online and offline realities, some of the consequences for not adopting appropriate cyberviolence definitions and policies result in shattering consequences to education and career opportunities, reputation, financial stability and assaults to physical, psychological, and emotional wellbeing. In professions where girls and women are in high profile fields and where progress and innovation is difficult to predict, such as in the virtual reality technologies sector, journalism, politics and academics, such consequences can be especially damaging, given the compounding threats to women and girls' rights. For girls and LGBTQQI2S and gender non-conforming young people, who participate in social networking, gaming and in navigating online spaces in which cyberviolence occurs, staying safe can be challenging. Therefore, having policies in place that acknowledge their unique experiences can both de-normalize sexual and gender based cyberviolence and support people when it occurs. It is imperative that organizations develop clear definitions, guidelines, and strategies for preventing and addressing cyberviolence; by not doing so, these organizations risk giving off the message that cyberviolence is acceptable and even tolerated, and open themselves up to costly and damaging legal repercussions.

By working with stakeholders to develop policy and best practices, the Atwater Library and Computer Centre's Preventing Cyberviolence Project aims to ensure that these organizations become allies in creating a safe and secure space for all of their participants, students, employees, families, and their community partners.

Prologue

Changing cultural perceptions that view gender based cyberviolence as normal or as a form of entertainment will be more challenging than merely enacting policy or legislation (Atwater Library and Computer Centre's Preventing Cyberviolence Project).

While developing strong, relevant and effective legislative solutions are essential, we also support strategies that empower our stakeholders to implement definitions, policies, practices and mechanisms that prevent and respond to cyberviolence and support people who have experienced it.

We suggest that both legislative and policy solutions will be most effective when acknowledging and actively addressing the gendered, racialized, and sexualized nature of online violence.

1. The Atwater Library and Computer Centre's Commitment to Working Against Cyberviolence

1.1 Participatory and Inclusive Collaboration on the Definition of Cyberviolence:

Cyberviolence refers to online or technology facilitated behavior that constitutes or leads to harm against the psychological and/or emotional, financial, physical state of an individual or group. Although cyberviolence occurs online, it can begin offline and/or have serious offline consequences. Gender-based cyberviolence, specifically, refers to the cultural and social norms, behaviors and standards that allow women, girls, LGBTQQI2S[1] *and gender non-conforming people to be targets of violence, inequality and misogyny in both online and offline worlds.*

This definition is the result of ongoing contributions from the stakeholders involved in the Atwater Library and Computer Centre's Preventing Cyberviolence Project. We strongly advocate for a participatory process in which stakeholders can draw upon the framework and recommendations we have collaboratively developed, to adopt definitions and create policies and practices that reflect the unique needs, identified problems, and socioeconomic contexts of their organizations and communities.

1.2 Rationale for Strategy:

The findings from our needs assessment (April, 2014) pointed to a need, on the part of stakeholders, for a clear definition of cyberviolence directed at girls and women, LGBTQQI2S and gender non-conforming people.

In the absence of clear definitions and policy that consider the gendered nature of cyberviolence, our stakeholders warned us that it was nearly impossible to prevent and eliminate this phenomenon within their organizations. Clear definitions and policies were found to be integral to addressing cyberviolence for a variety of reasons. For one, having concrete definitions and policies in place will allow stakeholders to send a clear message to their communities that gender-based cyberviolence is not tolerated. Moreover, definitions

[1] Lesbian, Gay, Bisexual, Trans, Queer, Questioning, Intersex, and Two-Spirit

can be effective in shining the spotlight on cyberviolence, and, in so doing, can 'de-normalize' the practice for both victims and perpetrators. Perhaps most importantly, clear definitions serve as tools for those targeted by cyberviolence, in particular, girls and women, LGBTQQI2S, and gender non-conforming people, who continue to experience obstacles when accessing support and resources.

Many of our stakeholders have experienced cyberviolence. Too often, their workplace, administrations, employers, teachers, counselors, colleagues, family and friends did not know how to address the problem and how to find appropriate resources. The lack of awareness about the harmful effects of cyberviolence often lead to their experiences being trivialized, normalized, and dismissed as just something that happens when you go online or use technology. Among these shared stories, survivors of cyberviolence feeling responsible for the violations, and feeling blamed for having made themselves visible in an online space where violence occurs. This is referred to as victim blaming and research reveals that it is an all too common response among people who report incidences of cyberviolence to authorities[i]. The danger in this pervasive response from service providers is that it discourages victim reporting and removes responsibility from the perpetrators, and places their actions back onto the victims. Indeed, some recommend, that, in lieu of victim blaming, it is more prudent to create harm-reduction strategies where education is at the forefront of the solution to ending cyberviolence[ii].
Therefore, developing and adopting clear definitions, policies, tools and resources that effectively respond to cyberviolence and center around survivor support is so crucial to ending cyberviolence once and for all

1.3 Objectives

The goal of this strategy is to work with our stakeholders in education, academia, law enforcement, health, counseling and the video game and technology industries to develop, adopt and implement clear definitions of cyberviolence, policies to prevent cyberviolence, and to consider potential responses to and consequences for acts of cyberviolence, along with resources for individuals who experience cyberviolence.

Due to the continuously evolving nature of technology, we endeavour to craft definitions and policy recommendations that focus on people, organizations, and communities, rather than solely on specific technologies. Our partner organizations require broad policies that can be adapted based on individual needs, environments and circumstances; they require policy strategies that are easily implemented and that account for the contextual and ever changing technological and social landscape in which cyberviolence occurs. Our aim is to provide tools for individuals and groups that address codes of behavior that they can apply to a variety of platforms and communication spaces as online environments evolve.

1.4 Procedure for the strategy:

- We are conducting an extensive literature review to find existing cyberviolence definitions, policies and recommendations to build a resource database that will be widely available online
- We are working with individual stakeholders to understand their specific and contextual needs with regards to definitions, policy, and resources

- We are helping stakeholders to strengthen and expand upon existing policies by assisting them in examining and evaluating the effectiveness of their current policies, practices and protection mechanisms
- We are collaborating with stakeholders in developing, refining, and sharing resources
- We are assisting stakeholders (who have no pre-existing definitions and policies in place) to develop and implement policy and resources that fit the needs of their organizations
- We are collaborating with stakeholders in knowledge mobilization around the social issue of cyberviolence, 'de-normalizing' cyberviolence, and specifically, in acknowledging the gendered, racialized, and sexualized nature of cyberviolence

1.5 How do we define cyberviolence?

The United Nations defines violence against women as including "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts."[iii] Unfortunately, there is no agreed upon international legal definition of cyberviolence, specifically, at the present moment. However, the United Nations Broadband Commission for Digital Development, in its recent report entitled *Combatting Cyber Violence Against Women & Girls: A Worldwide Wake-up*[iv], stresses that cyberviolence is an online extension of this definition and includes acts like trolling, hacking, spamming, and harassment.

Combining definitions of gender-based violence with cyberviolence are all too often critiqued as being 'too vague' or 'too broad'. However, due to the multi-faceted and wide-ranging ways that gender-based cyberviolence plays out, definitions need to be broad enough to encompass both existing and emerging manifestations.

The Atwater Library and Computer Centre, in collaboration with their stakeholders defines cyberviolence as:
Any online or technology facilitated behavior that constitutes or leads to harm against the psychological and/or emotional, financial, physical state of an individual or group. Although cyberviolence occurs online, it can begin offline and/or have serious offline consequences. Gender-based cyberviolence, specifically, refers to the cultural and social norms, behaviors and standards that allow women, girls, LGBTQQI2S[2] and gender non-conforming people to be targets of violence, inequality and misogyny in both online and offline worlds.

As society increasingly embraces new forms of technologies and communication, it becomes evident that institutions and industries need to address cyberviolence through proactive policies. Students and members of the workforce, for example, have the capacity to access the internet from their personal devices at anytime from anywhere; this means that there is potential for cyberviolence to occur both during and after school and work hours. The concern is that as cyberviolence becomes increasingly pervasive, it becomes increasingly normalized and embedded in the fabric of our society.

[2] Lesbian, Gay, Bisexual, Trans, Queer, Questioning, Intersex, and Two-Spirit

1.6 Normalization of cyberviolence

The question is often raised as to why cyberviolence against women, girls, LGBTQQI2S and gender non-conforming people matters, when there is so much violence against these groups offline. How can incidents that occur in virtual spaces be just as relevant as those that occur in physical spaces? Research demonstrates that for many people today, and particularly for youth, there is no online/offline divide[v]. Virtual spaces pervade every aspect of life as we are continuously connected to the internet, to our online communities, and to each other.

The physical, psychological, emotional and financial consequences of our online experiences can be profound and are experienced both on and offline. In our research, stakeholders expressed that online violence normalizes offline violence[vi].Being immersed in a digital culture that portrays sexualized violence, misogyny, the objectification of women, hyper-sexualisation of girls and discrimination against LGBTQQI2S and gender non-conforming people as normal, as entertainment or as humour, makes those representations and beliefs seem mainstream, palatable, and acceptable in offline environments. In effect, normalization of gender-based, sexualized cyberviolence contributes to perpetuating rape culture where both men and women assume that sexual violence is an inevitable fact of life.

The online environments and communities we interact with are important and have implications for our offline lives. As technology becomes more and more a part of our everyday lives, and as designers and developers seek to make our online interactions more powerful and realistic (e.g. the development of virtual reality technology), it is ever more critical to ensure that those technologies are developed and integrated into our lives in meaningful and ethical ways.

2. The costs of cyberviolence

The Atwater Library and Computer Centre's Cyberviolence Prevention Project works in partnership with a variety of institutional and industry stakeholders. We are increasingly invited to address the growing number of cyberviolence cases occurring in schools, colleges and universities, as well as community organizations, private corporations and industry.

2.1 Social Costs of Cyberviolence in Society, Schools and the Workplace

The Cyberviolence Prevention Project encourages its partners to examine the effectiveness of their existing policies, practices and protection mechanisms against online violence and in addressing its associated costs, whether they be social, psychological, legal, economic and/or emotional in nature.

2.1.1 Real People, Real Lives

The increasing use of the Internet in people's everyday lives, along with other forms of technologically facilitated communication, has had the effect of blurring the boundaries between people's online and offline realities. The impacts of online violence are felt offline and can have profound impacts in survivors' lives, leading to potentially devastating consequences to education and career opportunities, reputation, financial stability and physical, psychological, and emotional wellbeing. While the Internet and new technologies provide unprecedented opportunities, we are also facing previously unanticipated challenges

in the form of cyberviolence. It is crucial that we address the issue of cyberviolence through acknowledging and defining the issue, developing and implementing legislation and policy, outlining best practices and promoting educational initiatives that de-normalize this harmful practice.

2.1.2 Thinking forward – the impacts of emerging technologies

Collaborating with video game, virtual reality and social media industry to anticipate and attempt to avoid potential forms of cyberviolence relating to emerging technologies is integral in developing effective legislation and policy moving forward. With virtual reality, for example, comes more graphic, realistic enactments of sexual and gendered violence that can adversely and profoundly impact girls' and women's sense of safety, self-worth, and dignity. When developing legislative and policy strategies, it is imperative to project forward and plan for the emergence of new technologies and manifestations of cyberviolence. No one can predict exactly how technology will evolve or how people will adapt to it. Nonetheless, there are certain developments that we are aware of and can plan for accordingly, namely the oncome of virtual reality technologies. In addition to becoming increasingly immersive and realistic, this form of technology poses new threats to women's and girls' rights[vii].

2.1.3 Cyberviolence has the potential to limit the online participation of girls and women, LGBTQQI2S and gender non-conforming people

Increasingly, girls and women in high profile fields, such as journalism, politics, academics, video game and technology industries, have reported being targets of virulent cyberviolence. They endure a wide-range of harassment from graphic rape and death threats, doxing, defamation, to coordinated denial-of-service attacks and "image reaping" campaigns to shut down victim's websites and blogs. This online misogyny and gender-based cyberviolence does not only result in the target potentially censuring their online participation, shutting down accounts or going offline, it also serves as a highly visible example to all girls and women of what can happen when you stand out or "lean in" either online or offline spaces. During the course of this project, we have witnessed feminist academics and video game scholars and designers being publically targeted. This resulted in girls and women in their fields closing LinkedIn accounts and their blogs in order to avoid being noticed and further targeted.

There are countless examples of girls and women's intimate photos being shared without consent, images or videos of sexual assault being distributed, sexual assault threats being incited, women and girls being groomed and lured online for the purpose of human trafficking and exploitation, and LGBTQQI2S and gender non-conforming people being harassed or targeted online because of their sexuality and/or identity[viii]. The enactment of this type of cyberviolence risks significantly reducing the online participation and contributing to the marginalization of these groups.

2.1.4 The impacts of cyberviolence

Girls and women experience a myriad of personal, economic and social costs when they limit and/or censure their online participation to avoid cyberviolence. As highlighted by the RCMP in the online document entitled: Bullying and Cyberbullying[ix], the effects of

cyberviolence on students and employees may also potentially include:

- depression, social anxiety, loneliness, isolation, stress related health problems (e.g., headaches, stomach aches) and low self-esteem
- school and work absenteeism
- academic and professional performance problems
- aggressive behaviours
- contemplating, attempting, or committing suicide

By not having clear policies and practices in place against cyberviolence, the perceived message that institutions and industries are sending is that cyberviolence is an acceptable form of social interaction within their communities.
The refusal to act or to be fully committed to implementing anti-cyberviolence policies and practices can also affect communities at large. Cases of cyberviolence can result in an increase in[x]:

- Delinquent behaviour and substance use
- Professional or academic problems
- Increase in school dropout rates or employment terminations
- Aggression, sexual harassment, dating aggression
- Illegal activities, including gang involvement and criminal sanctions

These consequences highlight the critical need for institutions and workplaces to respond by implementing effective action plans.

2.2 The Legal Costs of Cyberviolence

Law enforcement agencies and their personnel often face challenges when attempting to determine their role in addressing cyberviolence. The rapidly emerging and evolving forms that cyberviolence can assume compounds the issue, which will require extensive research to develop contextual and nuanced legislation to effectively respond to cyberviolence.

2.2.1 Canadian Criminal Code's, Role in Preventing Cyberviolence

While the justice system struggles to learn how to best apply existing laws that are often drafted well before digital technologies reach current cultural pervasiveness, to emerging acts of cyberviolence, the Canadian Criminal Code[xi] fails to contain Acts that effectively prohibit many forms of cyberviolence.
Further, as we are in the earliest stages of attempting to legislate against cyberviolence, it remains uncertain how effective the response of a justice system will be to continuously changing manifestations of cyberviolence. However, depending on the nature of certain online activities, some violent acts that are potentially committed online are considered unlawful and can result in criminal sanctions and imprisonment[xii], such as:

- criminal harassment, uttering threats, intimidation
- mischief in relation to data, identity fraud, extortion
- false messages, indecent or harassing telephone calls
- counselling suicide

- incitement of hatred, and defamatory libel

In 2014, the Government of Canada passed the Protecting Canadians from Online Crime Act[xiii] that amended the Canadian Criminal Code to reflect the changing nature of cyberviolence in Canada. As a consequence, it is illegal[xiv] to share and distribute intimate or sexual images or videos of a person without their consent. A common example of this illegal practice is revenge porn, where intimate images, photographs and videos of sexual acts are posted on social media or on pornography websites. Judges now have the authority to order the removal of unauthorized images from the internet, and sanction the author of the crime.

Although there exists no obligation to report a suspected crime under Canadian law, institutions and employers must report any crime that has been witnessed or shared. Failure to comply and report cyberviolence to the authorities or designated agencies can result in criminal sanctions under Section 22 and 22.1 of the Canadian Criminal Code[xv], consistent with aiding or abetting the crime to take place.
Institutions and industry that knowingly turn a blind eye or suppress information related to an online crime can also be held criminally responsible; failure to report the crime of cyberviolence can lead to the institution or industry and its members to be personally held liable.

2.2.2 Professional Obligations to Report a Crime

Under each provincial and territorial professional order relating to social services and academic institutions, there may exist an obligation to report a crime. In Quebec, Sections 38 (2) c) and 39 of the Youth Protection Act[xvi] can be interpreted as creating an obligation for professionals working with children and adolescents to report the crime of cyberviolence. The act protects against any psychological ill-treatment of a child by the parents or another person in schools, institutions and related activities. For example, a teacher who has, a) informed the student's parents that there are reasonable grounds to believe that the psychological wellbeing, security or development of their child is in danger through cyber-violence and cyber-bullying and, b) the parents have failed to take the necessary steps to rectify the situation, has a professional obligation to inform the Director of Youth Protection concerning the incident.

2.2.3 Cost of Cyber-Harassment in the Workplace

Each province and territory in Canada has its own laws governing behaviours in workplaces. It is important to have a clear understanding of the labour laws that are applicable to your particular institution or company. Common trends exist when dealing with the employer's responsibilities to maintain a work environment free of violence and harassment, which can include sexual, physical and psychological acts that are:

- vexatious, repeated, and serious, hostile or unwanted by the employee
- affect the dignity or physical or psychological integrity of the employee
- create a harmful work environment

With the advancement of technological communications, the changing nature of employment and the use of the internet in the workplace, institutions and companies are

being forced to examine impacts and legal responsibilities relating to cyber-harassment and cyberviolence.
Provincial and territorial laws provide mechanisms for employees to file complaints against employers based on their rights to work with dignity and without online violence from management, other employees and clients. Examples could include:

- sexual, threatening and demeaning emails sent to intimidate or reinforce a verbal attack
- posting inappropriate content on work Facebook page
- using personal Facebook networks to circulate false, negative, and harmful information about another employee.

The institution or company can be held responsible for these acts if the offense occurred during the conditions of work employment or if it is directly related to an activity, event, and/or obligation organized by the workplace. This can result in various legal costs of representation, costs relating to compensation and damages, and various other costs relating to the potential re-integration of the employees in the workplace.

3. Not Addressing Cyberviolence can Have Financial Impacts
The social and financial costs of inaction can foster an education or employment environment ripe with distress and conflict, often leading to the breakdown of wellbeing and trust. Cyberviolence in the workplace or institution can reduce productivity, increase associated medical costs, and irrevocably damage the reputation of the company or institution.

3.1 Productivity Decreases Because of Cyberviolence
The economic cost associated with cyberviolence is similar to other forms of violence in workplaces or institutions. However, cyberviolence is increasing and becoming more pervasive in everyday interactions, and it is often less visible than physical violence. Therefore, the negative effects of cyberviolence can be present and damaging for extensive periods of time before the cyberviolence becomes apparent or is reported to. Examples of costs include a decrease in productivity and earnings, lost time and reduced returns on investments in social capital. This affects the wellbeing of employees, can create an atmosphere of fear and intimidation and strain relationships with other institutions, suppliers and companies. Acknowledging that cyberviolence exists and is not tolerated within an organization, as a first step, arguably leads to earlier reporting and quicker resolution of incidents.

3.2 Medical Costs Increase Because of Cyberviolence
There are also costs associated with medical leaves of absence and increased insurance claims due to cyberviolence. Although research on the long-term medical effects of bullying seem to focuses on non-virtual bullying[xvii], similar impacts could be present during an episode of cyberviolence. Consequences to survivors will often include not being able to participate in work life and work-related activities based on medical issues related to isolation, stress, depression, fear and other illnesses[xviii].

3.3 Negative Corporate Image and Potentially Disastrous Public Relations Issues

How institutions and companies respond to cyberviolence can have a devastating and long-term impact on their reputation and potential future revenues.

Negative media coverage of an institution, or company's failure to protect and support survivors of cyberviolence, affects reputation and community buy-in. With more clients using the internet to make decisions, bad feedback and poor reviews through social media[xix] can paralyze membership and directly reduce revenue. After a public case of cyberviolence, additional funds must be spent on ways to communicate how the institution or company is taking positive steps to address the situation to support survivors. That is why it is important for companies and institutions to recognize the risks and costs of cyberviolence, because once recognized, risks can be mitigated through proactive policies and best practices, such as clear definitions, implementation of policies, member support, and training.

4. Conclusion: Proactive Policies on cyberviolence can Limit Risks and Associated Costs

Too often, cases of cyberviolence come to the attention of the administration of an institution or company following repeated human rights violations or immense tragedy. People experiencing cyberviolence may be reluctant to report the issue because of embarrassment, fear of not being believed, and uncertainties associated with their reputation.

In the absence of concrete policies, as well as meaningful and accessible support, the experience of cyberviolence can leave people feeling humiliated, isolated, and devastated in light of the far-reaching, negative effects it has on one's personal, economic, and professional realities. Victim blaming is also a common response to cyberviolence and discourages reporting. To mitigate these consequences, administration and management can take a proactive policy stance against cyberviolence, and provide guidelines that support gender equality and human rights among its members and employees.

In cases where clear definitions, policies, practices and protection mechanisms do exist, survivors of cyberviolence are more likely to find justice and to access proper support. Ultimately, this reduces the social, legal and economic costs associated with this crime. However, in instances where policies and practices are either unclear or non-existent, institutions far more likely fail to respond inappropriately or gravely mismanage cyberviolence cases, both of which increases further risks of re-victimization among survivors. As a result, the institution or workplace can be held responsible for failing to uphold their obligation to protect, and may face legal, social, and economic repercussions.

The best defense against costly complaints, legal proceedings, tragic social consequences and economic loss is to implement a strong proactive policy and action plans against abusive behaviour. A clear policy against cyberviolence, training for staff and members, practices promoted by management to prohibit violence, and protection mechanisms for potential victims and survivors can reduce risks. These steps are some ways institutions and companies can demonstrate and carry out their commitment to fostering environments free of cyberviolence.

In other instances, too often institutions and workplaces focus on fixing the problem of cyberviolence, after the fact, instead of taking a proactive and preventative stance on the issue. Developing and implementing clear policies and public education campaigns, along with making resources accessible to vulnerable groups, are some strategies organizations can use in striving for a more preventative approach. Such efforts can greatly benefit organizations given the low costs associated with prevention, in the short and long run.

However, it is important for organizations to recognize that solely reactionary interventions are ineffective and inefficient in addressing the fundamental causes of cyberviolence.
It is anticipated that this information will encourage our partners to take a look at their existing policies and practices and take active, preventative measures against cyberviolence. This includes an evaluation of the potential costs associated with their current policies and practices and implementation of solutions to strengthen their capacity to protect against cyberviolence. The Cyberviolence Project of the Atwater Library is available and willing to assist any organization or company with this process.

4.1 Potential Questions for Consideration when Drafting Policies, Procedures, Protection Mechanisms, and Prevention Activities Against Cyberviolence

As a starting point, below are some questions to consider when creating or adapting policy or when evaluating the effectiveness of your existing policy, practices and protection mechanisms addressing cyberviolence.
Note: This is a non-exhaustive list and not all of the questions or points will be relevant to your organizations particular needs:

- Do you have a clear definition and prohibition of cyberviolence?
- Does your policy adopt a flexible definition of technology-facilitated cyberviolence? Please consult Appendix I for a non-exhaustive list of cyberviolence.
- Does the policy address cyberviolence regarding the on-campus/off-campus interactions between students or colleagues and/or the at-work/after-work interactions between colleagues?
- Does your policy promote safer spaces for women and girls, LGBTQQI2S, and gender non-conforming people, boys, men, and the community at large?
- Were policies and practices developed through an inclusive and participatory process with relevant input from community members and stakeholders?
- Does this policy explain the different national and provincial laws?
- Does your policy include information on your organization's approach, complaint procedure, and methods for conducting investigations?
- Are your policies, practices, and protection mechanisms written from a human rights and survivor centered perspective? Are they designed to minimize fear of reprisals through, for example, anonymous reporting?
- Does your definition promote gender-inclusive language?
- Are complaints taken seriously and acted upon promptly? Is there a comprehensive intervention strategy that addresses incidents of cyberviolence that include

appropriate and timely responses? If not, what are the barriers and how could they be changed?

- Does the policy clearly define the role and responsibilities of the investigator? Is the investigator independent, neutral, objective, and knowledgeable of the law, policies, and practices? Do possibilities of conflict of interest or abuse of power exist?[xx]
- Are the findings of the investigation reported to someone with sufficient authority to enforce them? Are there requirements that assure that findings are presented in a timely and fair manner?[xxi]
- Are there guidelines for the reporting process? Does it specify that the report must summarize the allegations, steps were taken during the investigation, or what evidence should be gathered for each allegation?[xxii]
- Do the parties in the investigation have the right to representation, from such persons as a union steward, student union, ombudsperson, or legal counsel?
- Is confidentiality protected throughout the entire process? What mechanisms are present to ensure that information is only shared on a need-to-know basis, and only by interested parties?
- Do you have a protocol developed outlining how you will provide support and resources to the victims of cyberviolence after investigations have concluded?
- Do you have information and resources available for victims of cyberviolence?
- Does your policy provide guidelines, funding and measurable results/outputs for improving on future prevention activities?
- Does your policy effectively refer to and make connections with existing policies in place such as, an anti-harassment policy, safer spaces policy, or codes of conduct?
- Does your policy provide guidelines on how to include anti-cyberviolence messaging in promotion material? (E.g. handbooks, websites, support materials for counselling and development or human resource departments, bulletin boards, posters, etc.)
- Does your policy assign responsibility to a human resource contact person for the monitoring and evaluation of the effective implementation of the policy? Are adequate resources available to this person?

Appendix I

Manifestations of Cyberviolence Developed with Stakeholders

¨Grooming – using social media to develop trust for the purposes of harming others (i.e. commit sexual assault)
¨Surveillance/Tracking – stalking and monitoring a victim's activities (i.e. GPS, Keystroke monitoring)
¨Recording and/or distributing images or video of sexual assault
¨Inciting others to assault
¨Distributing sexual images without consent
¨Harassing victims of sexual assault
¨Violent threats (rape, death, etc.)
¨Distribution of doctored photographs
¨ Impersonation of the victim
¨ Identity theft
¨Lies and slander spread online about the victim with the intention of damaging the victim's reputation (libel)
¨Technical sabotage and privacy invasions such as hacking victims' computers, e-mail, social media accounts
¨Strategically sharing hacked information with the intention of manipulating the victim's life (this is particularly damaging if the victim is unaware that they are being targeted)
¨ Doxing (hacking and posting confidential information, such as social security numbers, medical records, passwords, license numbers, and banking information)
¨Distributing and sharing personal information online, such as home addresses, places of work or school, daily routines, and personal schedules
¨Defamation (posting or directly sending false information to a victim's friends, relatives, employers, or potential employers, with the expressed intention of permanently destroying the victim's reputation
¨Creep shots (clandestine or lewd photos taken of girls and women without their consent or knowledge, after which they are posted online without the individual's consent)
¨ Coordinated denial-of-service attacks and "image reaping" campaigns aimed to shut down victim's websites or blogs

Appendix II

Abuse Tactics

¨Gas lighting¨ (presenting false information with the intent of making victims doubt their own memory, or clouding their perception of their own mental well-being)

¨Dog piling¨ (A group of people overwhelming someone with a flood of unfriendly responses by posting successive comments in a short time period

¨Sea lioning¨ (pestering a target with unsolicited questions delivered with a false air of civility/a swarm of seemingly random, largely-anonymous, people descending to comment and criticize)

¨Gish galloping¨ (flooding a debate space)

References

[i] Suarez, E., & Gadalla, T. M. (2010). Stop blaming the victim: A meta-analysis on rape myths. *Journal of Interpersonal Violence*, *25*(11), 2010-2013.

[ii] Shade, L. R. (2016). Sexting panic: rethinking criminalization, privacy, and consent. *new media & society*, *18*(4), 686-688.

[iii] United Nations, General Assembly, December 20, 1993, Declaration on the Elimination of Violence against Women. Retrieved from http://www.un.org/documents/ga/res/48/a48r104.htm

[iv] UN Broadband Commission for Digital Development Working Group , 2015, Cyber Violence against Women and Girls a World-Wide Wake-Up Call, Retrieved from http://www2.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

Charlotte Alter, September 24, 2015, U.N. Says Cyber Violence Is Equivalent to Physical Violence Against Women. Retrieved from http://time.com/4049106/un-cyber-violence-physical-violence/

[v] Hirzalla, F., & Zoonen, L. V. (2011). Beyond the online/offline divide: How youth's online and offline civic activities converge. *Social Science Computer Review*, *29*(4), 481-498.

[vi] Soraya Chemaly, 19/09/16, Hate Crimes in Cyberspace" author: "Everyone is at risk, from powerful celebrities to ordinary people", Retrieved from: http://www.salon.com/2014/09/02/hate_crimes_in_cyberspace_author_everyone_is_at_risk_from_the_most_powerful_celebrity_to_the_ordinary_person/; Global Funds for Women, 19/09/16, Online violence: Just because it's virtual doesn't make it any less real Retrieved from :https://www.globalfundforwomen.org/online-violence-just-because-its-virtual-doesnt-make-it-any-less-real/; Jac sm Kee, 15/09/16, Malaysia, Building a Feminist Internet, Online Safety is often overlooked in the fight against gender based violence, Retrieved from http://ignite.globalfundforwomen.org/gallery/building-feminist-internet

[vii] Bianca Baldo, 2016-09-19, Virtual reality pornography and tech-related violence against women: To boldly go have sex where no one has done it before! Retrieved from http://www.genderit.org/feminist-talk/virtual-reality-pornography-and-tech-related-violence-against-women-boldly-go-have-sex

[viiiviii] Bianca Baldo, 2016/09/19, Protecting the right to freedom of expression: Strategies of survivors of tech-related violence against women, Retrieved from http://www.genderit.org/articles/protecting-right-freedom-expression-strategies-survivors-tech-related-violence-against-wome

[ix] Government of Canada, Royal Canadian Mounted Police, 2016-06-14, Bullying and Cyberbullying, Retrieved from http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm

[x] Ibid, Retrieved from http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm

[xi] http://laws-lois.justice.gc.ca/eng/acts/C-46/

[xii] Government of Canada, 2015-11-20, What are the potential legal consequences of cyberbullying? Retrieved from http://www.getcybersafe.gc.ca/cnt/cbrbllng/prnts/lgl-cnsqncs-en.aspx

[xiii] Government of Canada, Department of Justice, 2016-06-17, Protecting Canadians from Online Crime Act, S.C. 2014, c. 31, Retrieved from http://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/page-1.html

[xiv] Government of Canada, Department of Justice, 2015-01-07, Cyberbullying and the Non-consensual Distribution of Intimate Images. Retrieved from http://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/p6.html

[xv] Government of Canada, Department of Justice, 2016-06-17, Criminal Code (R.S.C., 1985, c. C-46), Retrieved from http://laws-lois.justice.gc.ca/eng/acts/c-46/page-4.html#docCont

[xvi] Government du Québec, Publication Québec, 2016-04-01, Youth Protection Act, chapter P-34.1, Retrieved from http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/P-34.1#se:39

[xvii] Mark Dombeck, Ph. D, MentalHealthNet, 2007- 07-24, The Long Term Effects of Bullying, Retrieved from https://www.mentalhelp.net/articles/the-long-term-effects-of-bullying/

[xviii] Government of Canada, Canadian Center of Occupational Health and Safety, 2016-07-08, Bullying in the Workplace, Retrieved from https://www.ccohs.ca/oshanswers/psychosocial/bullying.html

[xix] Patricio Robles, (not dated) The True Cost of Bad Publicity, Retrieved from http://www.ereleases.com/prfuel/true-cost-bad-publicity/

[xx] Lauren M. Bernardi, 2011-05, Investigating Harassment Complaints: Ten Costly Employer Mistakes, Retrieved from https://www.hrpa.ca/Documents/PD/PD%202016/tencostymistakes.pdf

[xxi] Ibid. Lauren M. Bernardi, 2011-05, Retrieved from https://www.hrpa.ca/Documents/PD/PD%202016/tencostymistakes.pdf
[xxii] Ibid. Lauren M. Bernardi, 2011-05, Retrieved from https://www.hrpa.ca/Documents/PD/PD%202016/tencostymistakes.pdf