TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE

REPORT ON THE PREVALENCE OF TF GBV DURING THE 2023 PEI PROVINCIAL ELECTION & A POLICY RECOMMENDATION FOR PEI POLITICAL PARTIES

PRINCE EDWARD ISLAND | COALITION FOR WOMEN IN GOVERNMENT

Acknowledgement: Interministerial Women's Secretariat

Since varying degrees of violence continue to plague women's political participation, we are grateful for the opportunity the Interministerial Women's Secretariat (IWS) has provided to our organization. The IWS continues to support the PEI Coalition for Women in Government's efforts towards ensuring a safer campaigning environment for women.

Throughout the summer of 2022, the Coalition held several in-person and online campaign schools that taught prospective women and nonbinary candidates how to run a municipal election campaign. Several participants shared concerns about how to prevent and respond to technology-facilitated violence (TFV). At that time, all the Coalition could offer were anecdotal suggestions. One individual even dropped out before the workshop, citing fear of online harassment. Although door-knocking on Prince Edward Island is important, social media has become an essential campaigning tool. With the provincial elections slated for the following year, the Coalition wanted to research the prevalence and forms of technology-facilitated violence affecting women and gender-diverse candidates on the Island. The funding for this report was awarded in the fall of 2022. Shortly afterwards, the Coalition met with the presidents of the provincial political parties and asked whether they had a policy pertaining to cyberviolence prevention and response. No party had any such policy, aside from a member responsible for ensuring candidates' social media posts were inoffensive prior to the start of a campaigning period. All parties agreed that having a cyberviolence policy would be useful. This gap inspired us to develop a set of recommendations informed by researched best practices and local candidate interviews. Our policy template provides standardised rules on how parties can actively respond to and prevent TFV. This report aims to serve as a starting point to introduce the topic of technology-facilitated gender-based violence and its direct connection to women's political participation in Prince Edward Island.

Vocabulary and Definitions

Gender: Refers to the characteristics of women, men, girls, and boys that are socially constructed. This includes norms, behaviours, and roles associated with being a woman, man, girl or boy, as well as relationships with each other. As a social construct, gender varies from society to society and can change over time.[1]

Gender-based violence: Gender-based violence refers to harmful acts directed at an individual based on their gender. It is rooted in gender inequality, the abuse of power, and harmful norms. It disproportionately impacts women, girls, and Two-Spirit, trans, and non-binary people. It includes sexual, physical, mental, and economic forms of abuse inflicted in public or in private as well as "threats of violence, coercion, and manipulation.[2]

Gendered disinformation campaigns: The spreading of deceptive or inaccurate information that follows storylines which draw on misogyny and gender stereotypes.[3]

Information communications technologies: Diverse set of technological tools and resources used to transmit, store, create, share, or exchange information. These technological tools and resources include computers, the Internet (websites, blogs, and emails), live broadcasting technologies (radio, television, and webcasting), recorded broadcasting technologies (podcasting, audio and video players, and storage devices), and telephony (e.g. fixed or mobile, satellite and visio/video-conferencing).[4]

Technology-facilitated gender-based violence (TF GBV): Sometimes referred to as cyberviolence, this is any act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools that results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms. These are forms of violence that are directed against women because they are women and/or that affect women disproportionately.[5]

Psychological violence: Patterns of behaviour that cause fear by intimidation; threats of physical harm to self, partner, or children; destruction of pets and property; "mind games"; or forcing isolation from friends, family, school and/or work.[6]

---

[1] World Health Organization. (2019). Gender and Health.
[2]The UN Refugee Agency.(n.d). Gender-based violence.
[3] Montreal Institute for Genocide and Human Rights Studies.(2021). Canadian Women Leaders' Digital Defence Initiative Report
[4] United Nations Population Fund. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe Report.
[5]UN Women.(n.d). Frequently asked questions: Tech-facilitated gender-based violence.
[6] UN Women. (2022). Frequently asked questions: Types of violence against women and girls.

Violence against women: Any act of gender-based violence that results in, or is likely to result in, physical, sexual, or mental harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or in private life.[7]

Forms of Technology Facilitated Violence[8]

- **Cross platform Harassment:** The coordinated and deliberately deployed harassment against a target by a single harasser or a group of harassers, across multiple online communication platforms, who take advantage of the fact that most platforms only moderate content on their own sites.

- **Cyberstalking, Tracking or Pursuit and Surveillance:** The use of technology to stalk and monitor someone's activities and behaviours in real-time or historically.

- **Deadnaming:** A form of direct harassment in which a target's former name is revealed against their wishes for the purposes of harm. This technique is most commonly used to 'out' members of the LGTBQIA+ community who may have changed their birth names for any variety of reasons, including to avoid professional discrimination and physical danger.

- **Deepfakes**: Digital images, videos, and audios that are artificially altered or manipulated by AI and/or deep learning to make a person appear to do or say something they did not actually do or say. Deepfakes can be difficult to distinguish artificially manufactured material from actual videos and images. They are increasingly being used to create non-consensual sexual imagery that depicts the target in a sexual way, such as placing their faces in pornographic videos.

- **Defamation:** The public release of false information that damages a person's reputation and that has the intention of humiliating, threatening, intimidating, or punishing the target and in particular public figures such as prominent officials, activists, and journalists.

- **Doxxing:** Non-consensual disclosure of personal information. It involves the public release of an individual's private, personal, sensitive information, such as home and email addresses, phone numbers, employer and family member's contact information, or photos of their children and the school they attend, with the purpose of locating and causing physical harm.

[7] World Health Organization. (2019). Gender and Health.
[8] United Nations Population Fund. (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe Report.

- **Gendered hate speech:** Any kind of communication in speech, writing, or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in this case, based on their sex, gender, sexual orientation or gender identity. Gendered and sexist online hate speech reinforces systemic sexism while dehumanizing and encouraging violence against women and girls and LGBTQIA+ people.

- **Hacking:** Use of technology to gain illegal or unauthorized access to systems or resources for the purpose of attacking, harming, or incriminating another person or organization by stealing their data, acquiring personal information, altering or modifying information, violating their privacy or infecting their devices with viruses.

- **Image-Based Abuse (IBA):** The use of images to coerce, threaten, harass, objectify, or abuse a target. This involves taking, threatening to share, or sharing intimate and/or sexual images without consent.

- **Impersonation:** The process of stealing someone's identity to threaten or intimidate and discredit or damage a user's reputation. This does not include clearly identified parody accounts.

- **In-real-life (IRL) attacks:** Incidents where online abuse either moves into the 'real' world or is already part of an ongoing stalking or intimate partner violence interaction.

- **Mobbing:** Also called dogpiling or networked harassment, mobbing consists of organized, coordinated, and systematic attacks by a group of people against particular individuals or issues, for instance targeting feminists or people who post about racial equality issues online. Outrage or shame mobs are a form of mob justice focused on publicly exposing, humiliating, and punishing a target who often expresses opinions on politically charged topics or ideas that the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda.

- **Online Harassment:** A course of conduct that uses technology to repeatedly contact, annoy, threaten, or scare another person through unwelcome, offensive, degrading, or insulting verbal comments and often images, and is committed by single individuals or mobs.

Introduction

Over the past 20 years, online connectivity has rapidly expanded across the globe, and has increased since the onset of the COVID-19 pandemic. This resulted in the widespread integration of digital communications and relations into everyday life, and access to the Internet increasingly proves itself to be an essential component of civic engagement. Online forums, blogs, and social media platforms provide a space for individuals and groups to express ideas, engage in public discourse, and mobilize for a cause. Technology and the internet are not inherently bad, but unregulated safety policies and built-in human bias have facilitated new avenues for abusive behaviour.

Technology-facilitated violence (TFV), sometimes referred to as cyberviolence, is an accelerating global and local issue. This encompasses a wide range of aggressive behaviours that are enacted using information and communications technologies such as computers, cell phones, GPS tracking devices, and artificial intelligence. Facebook, Instagram, X (formerly Twitter), Snapchat, WhatsApp, and other popular social media platforms are the most common locations for incidents of cyberviolence.[9] While anyone can be the target of cyberviolence, women and girls, racialized people, and gender and sexually diverse people are disproportionately harassed. In particular, women who regularly engage in public online platforms, e.g. politicians, journalists, academics, and activists, face an additional risk of being targeted[10]. The ultimate goal of these attacks is to deter women from pursuing positions of leadership.

Academics, national and international governmental and non-governmental institutions are increasingly conducting research on the prevalence, characteristics, and mechanisms of technology-facilitated violence. The findings consistently demonstrate that TFV is an extension of traditional intersecting systems of oppression. The foundations of TFV can be understood as digital manifestations of sexism, racism, ableism, homophobia, and transphobia. In other words, vitriolic attacks unleashed on marginalised people through technology do not happen in a vacuum. If all digital technologies disappeared tomorrow, women and gender-diverse people would continue to experience gender-motivated hate because the root causes of this discrimination have not been eliminated. While the tools and techniques may be new, the motivations remain the same: to control, silence, scare, and attack women and gender-diverse people. It is important to remember that gender-based violence (GBV) pre-dates the internet. Society's collective failure to address systemic sexism is how TFV against women flourishes.[11]; it is proven that outrage and misogyny are profitable to social media platforms, giving them little to no incentive to adopt effective regulations.[12]

[9]Institute of Development. (2021). K4D Helpdesk Report: Global Evidence on the Prevalence and Impact of Online Gender-based Violence (OGBV)
[10]Council of Europe: The Commissioner's Human Rights. (2022). No space for violence against women and girls in the digital world.
[11]Khoo. (2021). Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence. Women's Legal Education & Action Fund.
[12]Jankowicz, N, et al. (2021). Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online.

With minimal recognition of technology-facilitated violence, the severity of online harassment is often downplayed and accepted as 'part of the job' for prominent leaders. This mentality is not helpful in combating TFV, and in fact, perpetuates the narrative that this form of violence must be accepted. According to the Canadian Women's Foundation, online threats of violence can evolve into in-person violence, contributing to significant safety concerns for women and gender-diverse people in society.[13] Victims largely lack the tools to prevent, respond to, and report technology-facilitated gender-based violence (TF GBV) beyond deleting or ignoring aggression. Suggesting that women log off, delete, or ignore the hate they receive does not address the issue. Whether they are a political candidate, elected official, or volunteer, politically involved women often do not have the choice to opt out of online spaces. Moreover, online visibility is an increasingly inescapable professional expectation for political candidates and elected officials to reach their constituents.

Identifying Technology-Facilitated Gender-Based Violence (TF GBV)

The first step in addressing this type of gender-based violence is to understand how to define and recognize the forms of TF GBV. Our technological landscape continues to rapidly evolve, and new configurations are constantly developing. A 2021 report from the United Nations Population Fund identified the following distinguishable characteristics of TF GBV:[14]

Anonymity
The perpetrator can remain anonymous.

Automation
Certain technologies have automated functions to distribute comments, images or track the movements of women with little effort on the part of the perpetrator.

Action at a distance
It can be perpetrated at a distance, from anywhere in the world, and without personal or physical contact with the target.

Accessibility and affordability
The acquisition of an individual's digital information is cheaper and easier to obtain than ever before.

Collectivity
Attacks against women online can easily be quickly coordinated to involve a mass number of people from around the world.

[13]Canadian Women's Foundation.(n.d). The Facts about Gendered Digital Hate, Harassment, and Violence.
[14]United Nations Population Fund.(2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe Report.

Normalisation of violence
TF GBV contributes to the normalisation of violence against women and girls; it is perceived as less serious or dangerous.

Perpetuity
Digital images and materials are likely to exist indefinitely within online spaces, and can easily be saved to the devices of perpetrators.

Propagation
Online content is easily reproduced, and accounts can be automated to re-share damaging images, messages, or other materials to consistently harass a target.

Impunity
Given that TF GBV can be committed anonymously and from a distance, this makes it difficult for law enforcement to hold abusers accountable; there are often no consequences for enacting this form of violence.

Statistics Regarding TF GBV Against Women Globally

Widespread technological connectivity has positive and negative impacts on the lives of women. An increased connection to the internet and mobile phones has provided some women with low barrier access to information and allowed for open avenues for them to utilize expanded educational and employment opportunities.[15] Despite these net positives, online platforms and technologies exacerbate existing forms of gender inequities and oppression.

The KD4 Helpdesk Report, Global Evidence on the Prevalence and Impact of Online Gender-Based Violence, summarizes findings of recent surveys across hundreds of countries from 2018-2021. While this report provides widespread data to assess global trends, different definitions of TF GBV, age ranges of participants, of sample sizes, and of regionally specific access to technology make comparing these results difficult.

That said, these large-scale studies do reveal the troubling frequency with which women and girls across the globe experience TF GBV. The criteria used to define TF GBV in the KD4 report identified the following;

- Plan International surveyed 14,000 girls and women ages 15-25 in 22 countries and found that 58% of respondents had experienced some form of online harassment on social media platforms.

[15]Institute of Development. (2021). K4D Helpdesk Report: Global Evidence on the Prevalence and Impact of Online Gender-based Violence (OGBV)

- The World Association of Girl Guides and the World Wide Web Foundation distributed a survey to 8,000 girls and women of all ages in 180 countries and found that 52% have experienced some form of online gendered abuse.
- Researchers Gurumurthy et al. administered an anonymous survey to 800 women ages 19-23 in six Indian cities and towns, finding that 31% of respondents experienced online sexual harassment.
- The American Pew Research Center surveyed 10,000 adults age 18+, including men, and found that 16% of women experienced online sexual harassment. 47% of the women who reported experiencing online harassment identified it as gender-based compared to the 18% of men who encountered harassment online because of their gender.

Technology-Facilitated Violence Against Women in Leadership

The Inter-Parliamentary Union, a globally recognized organization, studied 55 women parliamentarians from 39 countries in 2016 and found that 42% of respondents had been subjected to dissemination of comments and images via social media platforms about their personhood that carried sexual, defamatory or humiliating connotations, specifically relating to their gender. The majority of women parliamentarians surveyed reported experiencing some kind of psychological violence, including threats which were usually delivered through social media. Of the women respondents, 44% said they had received threats of death, rape, beatings, or abduction of them or their children. This risk of gender-based online harassment increased for women parliamentarians if they were; young, part of a minority group, or a member of an opposition party. Additionally, women who took up positions defending human rights or feminism were often targeted at higher rates.[16] This was the first time the Inter-Parliamentary Union conducted gender-based research into TF GBV against women parliamentarians. It is imperative this study be replicated to obtain more recent data, in the wake of the subsequent 'Shadow Pandemic', the term given to the uptick of violence against women and girls internationally since the onset of COVID-19.[17]

As in many other nations, organizations in Canada have only just begun researching the effects of TF GBV on women political leaders. One of the most recent reviews on the prevalence of online gender-based violence against women politicians was measured by the Montreal Institute for Genocide and Human Rights Studies. The Institute hosted a Canadian Women Leaders' Digital Defense Initiative in 2021 during which prominent women politicians and journalists were interviewed, and several recurring themes were identified.[18] The participants spoke to a growing amount of gendered online abuse and disinformation aimed at threatening and dehumanising women politicians and undermining their credibility. The researchers confirmed that racialized women politicians received more abuse, with many remarking that attacks were often driven by

[16]Inter-Parliamentary Union. (2016). Sexism, harassment and violence against women parliamentarians.
[17]Government of Canada. (2023). The shadow pandemic: combatting violence against women and girls in the COVID-19 crisis.
[18] Montreal Institute for Genocide and Human Rights Studies. (2021).Canadian Women Leaders' Digital Defence Initiative.

their political opponents, whose lack of civility encouraged their supporters to follow their lead. This tactic resulted in a legitimized tool to silence these women politicians.

These attacks were described by the women as traumatic. There was a collective worry that voicing their concerns publicly about this abuse would diminish their political credibility, and a fear that the attacks would increase or be more severe if actions were taken to address it. Most felt alone and unsure of how to navigate online attacks, and cited a lack of clear avenues of support and reporting from their political parties or social media companies. They were also frustrated by the futile prospect of holding perpetrators accountable. Ultimately, all women politicians and journalists who participated in the roundtable considered online harassment a strong deterrent and obstacle for women considering a career in politics, especially since maintaining an online presence is now essential for work.

One woman participant, Canadian senator Marilou McPhedran, stated that “Gender-based attacks against women in politics must be seen as efforts to undermine democracy and dealt with accordingly.”

Canadian federal and provincial political parties have a responsibility to create and maintain an environment that is civil to all. To ensure this happens, parties can use the technology-facilitated gender-based policy template, and commit to establishing guiding principles to navigate, address, and respond to technology-facilitated gender-based violence.

Methodology and Data

To begin reporting on the types and frequency of technology-facilitated violence within PEI, the PEI Coalition for Women in Government issued a preliminary survey to all 53 women and gender-diverse candidates registered in the 2023 provincial election. This survey allowed candidates to submit evidence of any instances of TFV experienced during their campaign. After responses were collected, debrief interviews with available candidates from all four political parties were conducted over a six-month period following the election results. Only three individuals completed the survey, however, twelve candidates agreed to a post-election interview. This resulted in a pool of fifteen women and gender-diverse candidates who described their personal experiences during the 2023 provincial election campaign period.

a) Violence on the Campaign Trail Survey

Taking an average of 10 minutes to complete, the survey contained five demographic-identifying questions and nine questions on the candidate’s experience. Although the response rate was low, 33% of women and gender-diverse candidates were subjected to an instance of technology-facilitated gender-based violence. For the individual who did report an instance of TF GBV, they provided screenshots of anonymous accounts that commented on their election-related posts over social media. These abusive comments were anonymous, and targeted their gender specifically, using both image-based abuse and gendered hate speech.

b) Post-election Debriefs

During the post-election interviews, definitions of what qualified as TFV varied greatly between individuals. Of the candidates we interviewed, 67% had experienced at least one form of TF GBV during the 2023 provincial election. This highlights the need for universal definitions and vocabulary of technology-facilitated violence to ensure widespread understanding and comprehension throughout our society by way of ongoing education.

Of the candidates who reported instances of technology-facilitated gender-based violence, the following themes emerged: they frequently did not report incidents of TF GBV to their party out of concern the party was ill-equipped to handle the incident, they expressed relief that their experiences did not escalate to in-real-life (IRL) attacks, and they learned there was often little the RCMP were able to do when they reported an incident.

As mentioned above, the Coalition spoke to women and gender-diverse people from all four political parties, each with their own unique backgrounds and perspectives. The experiences they reported ranged from messages and comments expressing anger about the party they were affiliated with to threatening personal attacks over social media. It is important to note that any messages directed at the political party but received by the women or gender-diverse candidates were not classified as TF GBV for the purposes of this report.

The PEI Coalition for Women in Government is grateful for the participation of the candidates who agreed to speak about their experiences in confidence. To ensure as much anonymity as possible, given the sensitivity of the interview content and the safety concerns that could arise, we have elected to use the pronouns they/them to refer to women and gender-diverse candidates, regardless of their gender identity. The privacy of the participants is of great importance to us. Below is a sample of anonymous quotes and descriptions of personal accounts of TFV from the PEI women and gender-diverse candidates who agreed to do a campaign debrief.

i. Anonymous Quotes & Responses

"*I did receive an anonymous threat over social media stating 'if you win your seat, you will regret it!'. A woman from the community also called me a 'murderer' for wearing a mask while I was campaigning. There was also a notable increase in troll accounts on Twitter* (troll/bot account: new accounts with little to no history on the platform).

"*A fellow candidate encouraged me to report the threat I had received to the local authorities, so I provided them with screenshots. I don't know if anything came of it.*"

One candidate was harassed on social media by a religious institution from outside of PEI, to which they had no prior connection to. The institution criticised them for running for a Party that supports abortion. The candidate did not report this incident to their party.

"I didn't even bother running any social media accounts for the recent campaign. In the past election, I received some aggressive comments that did nothing to further constructive policy dialogue on my Facebook Page."

One candidate received a hate comment from someone using a pseudonym. They recognized this pseudonym as it was used by someone they had a previous professional relationship with. This candidate later received an email from the suspected person confirming their hunch. They took screenshots of the comment and email and reported this encounter to an RCMP officer with whom they had a working relationship.

"*I used my own social media pages for the campaign, which was not recommended by the party, or by you folks* (PEI Coalition for Women in Government), *but there was no way I could build a brand new following in the time we had*."

" On election day I posted a photo of myself on my campaign Twitter account reminding everyone to vote. Under that tweet I received 35 separate replies from accounts questioning my mental stability and hate speech related to my gender. Someone either hired a bunch of Twitter bots to spam me with insulting replies and or an anti-mask/anti-LGBT+ group found me and decided to target me. Some of the Twitter accounts were from PEI but most were not local as far as I could tell. I didn't report it to the party, mostly because this incident happened on election day and I just ended up blocking or muting the accounts."

"I did get threatened. A guy must have found my personal email, I don't know how. There were thinly veiled physical violence threats, with a lot of cursing. I determined which district he was from so we avoided his house and the area. I was told to maybe call the RCMP, but nothing further."

"I'm not even sure we know how to identify when we (women) are being harassed online."

ii. Common Trends

Over half of the candidates interviewed reported at least one instance of TFV. These experiences were varied, across platforms and with known or unknown attackers. Many avoided using Twitter as a campaigning tool altogether, citing that "nothing beneficial could come" from having a presence on that platform. The candidates who were in favour of using Twitter explained that despite the increase of "troll accounts", the number of politically engaged constituents on that platform made it worth it.

For one individual, past negative experiences had driven them away from using social media during their campaign altogether. Most candidates we interviewed expressed feeling ‘lucky’ about their experiences with TFV. Even candidates who had negative experiences highlighted their gratitude that it never escalated to more severe forms, such as in person violence.

Political parties with larger resources and volunteer pools tended to have a separate person in charge of the candidates' social media. One candidate who had several staff assisting with their campaign, noted that their messages were “reviewed” before being presented to them. Another candidate hired a staff person to manage their social media accounts. These candidates did not report any instances of TFV during their campaigns. Comparatively, the candidates who managed their own social media accounts were more likely to receive and report instances of TFV, to both their personal and professional accounts.

Regardless of who managed the accounts, many candidates preferred using their personal social media profiles to engage with their community while campaigning. They reasoned that it provided them more control to filter people via friend requests, and allowed them to better protect their privacy. They featured family photos on their Facebook as a conscious effort to safeguard against any unwanted flirtatious behaviour. Another candidate felt uncomfortable with the volume of friend requests they received to their personal Facebook account; they preferred to keep their political life separate from their personal life.

Although much of the TFV these individuals experienced was not strictly focused on their gender, there were three notable instances which would be classified as technology-facilitated gender-based violence (TF GBV).

> The first candidate received several threatening and cruel comments over social media, including messages instructing them to visit a mental institution, and insinuating they should die because of their gender.
>
> The second candidate received an email from a constituent after they had spoken to him at his door stating, *“I would encourage you* (the candidate) *to focus on families and family resources, particularly those with young children,*”and that they should “*consider focusing on your family”* instead of running.
>
> The third candidate was repeatedly called ‘a bitch’ across social media platforms throughout their campaign, while other candidates in conversation referred to her stance on issues as “cute”.

The importance of broadening the scope of this work on Prince Edward Island cannot be understated. This report found that a rate of 67% of women and gender-diverse

candidates experience technology-facilitated violence. This high rate is significant enough that the Coalition recognizes the need for further study and the inclusion of different levels of government. The participation of all underrepresented genders in politics is necessary for a functioning democracy.

This report is an important starting point in analysing the emerging topic of technology-facilitated gender-based violence. The PEI Coalition for Women in Government aims to provide education and awareness on this topic, as it is a proven barrier to women's political participation. The policy template for PEI's provincial political parties is a necessary addition to their safety procedures, and should they choose to adopt it, will demonstrate their continued commitment to engage and retain underrepresented genders within their organizations. Technology-facilitated violence is challenging our democracy, but with continued education, study, and actionable changes, our society can mitigate and address this barrier to create a stronger and more inclusive political environment for all.

Summary of Policy Recommendations

- **Education:** Teach all candidates, campaign teams, and volunteers the definition of technology-facilitated violence to ensure they know how to identify it. Provide social media training and how to use the most relevant platforms, especially those platforms on which the party has an established presence. Training should emphasise when to block, delete, mute, or reply to comments and messages, and explain the benefits and repercussions of these decisions.

- **Standardised codes of conduct for online interactions:** Publicly list the guiding principles set by the party or individual to identify and manage interactions. Should a candidate face pushback from a citizen for blocking or deleting, refer them to the rule they violated.

- **Document and report:** Designate a person responsible within the party to receive reports of technology-facilitated violence, and establish a mechanism where candidates can submit screenshots and other evidence of the incident. Track the type and frequency of the technology-facilitated violence. Document each instance, including taking screenshots of the interaction with the date and time when possible.

- **Penalties:** Outline the consequences for individuals within the party who engage in technology-facilitated violence, such as fines, legal action, or expulsion from the party. Those on the receiving end should be allowed to pursue legal action if it is deemed necessary.

- **Support for victims:** Provide support and resources for victims of technology-facilitated violence, including access to counselling, legal assistance, and other support services.

Appendix A: Draft Technology Facilitated Violence Policy

1. **Scope**
    a. This policy applies to all candidates, members, elected-officials, staff, and volunteers of the _____ Party of Prince Edward Island.

    b. This technology-facilitated violence (TFV) policy applies to all online interactions and communications individuals from the Section 1(a) list have on behalf of the party or while engaged in party activities such as but not limited to; campaigning, volunteering, promoting, or fundraising.

2. **Purpose**
    The purpose of this policy is to set guidelines for how the _____ Party of Prince Edward Island will define, investigate and respond to instances of TFV against or perpetrated by its members.

    This policy does not prevent targets of TFV from seeking legal advice or reporting TFV cases to the authorities independent of the Party.

3. **Definitions**

    Technology-facilitated violence, sometimes referred to as cyberviolence, describes an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media. This includes the following behaviours:

a) **Cross platform harassment:** A coordinated and deliberately deployed harassment against a target, by a single harasser or a group of harassers, across multiple online communication platforms, taking advantage of the fact that most platforms only moderate content on their own sites.

b) **Cyberstalking, Tracking or Pursuit and Surveillance:** The use of technology to stalk and monitor someone's activities and behaviours in real-time or historically.

c) **Deadnaming:** A form of direct harassment in which a target's former name is revealed against their wishes for the purposes of harm. This technique is most commonly used to 'out' members of the LGTBQIA+ community who may have changed their birth names for any variety of reasons, including to avoid professional discrimination and physical danger.

d) **Deepfakes**: Digital images, videos, and audios that are artificially altered or manipulated by AI and/or deep learning to make someone appear to do or say something they did not actually do or say. They are becoming difficult to distinguish artificially manufactured material from actual videos and images. Deepfakes are increasingly being used to

create non-consensual sexual imagery that depict the target in a sexual way, for example, by placing women's faces on porn videos.

e) **Defamation:** Involves the public release of false information that damages a person's reputation and that has the intention of humiliating, threatening, intimidating, or punishing the target and in particular public figures such as public officials, activists and journalists.

f) **Doxxing:** Non-consensual disclosure of personal information. It involves the public release of an individual's private, personal, sensitive information, such as home and email addresses, phone numbers, employer and family member's contact information, or photos of their children and the school they attend, with the purpose of locating and causing physical harm.

g) **Gendered hate speech:** Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in this case, based on their sex, gender, sexual orientation or gender identity. Gendered and sexist online hate speech reinforces systemic sexism while dehumanizing and encouraging violence against women and girls and LGBTQIA+ people.

h) **Hacking:** Use of technology to gain illegal or unauthorized access to systems or resources for the purpose of attacking, harming or incriminating another person or organization by stealing their data, acquiring personal information, altering or modifying information, violating their privacy or infecting their devices with viruses.

i) **Image Based Abuse (IBA):** Using images to coerce, threaten, harass, objectify, or abuse a target. This involves taking, sharing, or threatening to share intimate and/or sexual images without consent.

j) **Impersonation:** The process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation. This does not include clearly described parody accounts.

k) **In-real-life (IRL) attacks:** Incidents where online abuse either moves into the 'real' world or is already part of an ongoing stalking or intimate partner violence interaction.

l) **Mobbing:** Also called dogpiling or networked harassment, consists of organized, coordinated and systematic attacks by a group of people against particular individuals or issues, such as by groups that target feminists or people who post about racial equality issues online. Outrage or shame mobs are a form of mob justice focused on publicly exposing, humiliating and punishing a target, often for expressing opinions on politically charged topics or ideas the outrage mob disagrees with and/or has taken out of context in order to promote a particular agenda.

m) **Online Harassment:** A course of conduct that involves the use of technology to repeatedly contact, annoy, threaten or scare another person through unwelcome, offensive, degrading or insulting verbal comments and often images, and that is committed by single individuals or mobs.

4. Responsibilities and Expectations

The Party will:

a. Offer social media and TFV training on an annual basis to candidates, volunteers and other members to allow them to identify and tackle TFV;
b. Develop a standardised code of conduct for online interactions by party members;
c. Publicly list the Party's guiding principles pertaining to online interactions;
d. Offer counselling, legal assistance, or other support services to members targeted by TFV.

The Provincial Council will:

a. Ensure they are informed with up-to-date information on identifying instances of TFV;
b. Receive reports of TFV perpetrated by or against a member of the Party;
c. Collect data on the type and frequency of TFV cases by and against Party members;
d. Support members of the Party should they block or delete citizens perpetrating TFV against them by referring the perpetrator to the Party's Technology Faciliated Violence Policy;
e. Escalate TFV cases to legal authorities should the violence include threats to the safety of its members.

Members will:

a. Undertake relevant social media and TFV training as offered by the party to remain informed on how to avoid perpetrating TFV, and how to deal with it if they or other Party members are targeted;
b. Document instances of TFV against themselves and other Party members, including screenshots and other relevant evidence;
c. Inform themselves about, and abide by, the Party's online code of conduct.

5. Process

A. Target of technology-facilitated violence

Should a member of the Party experience TFV as a result of carrying out their duties to the Party, including but not limited to as a candidate, volunteer or staff, they should:

I. Document evidence of the incident. This can include screenshots, audio or video recordings;

II. Set boundaries: block or report the perpetrator, and delete violent comments or posts once they have been documented;
III. Report the incident to the Provincial Council: include as much detail and specific evidence as possible.

The Provincial Council shall:

a. Designate a member of the Council to investigate instances of TFV and report back to the Council;
b. Provide a response to the targeted person within 30 days of the initial report being filed. This response should include:
    i. Confirmation of receipt,
    ii. Actions taken by the responsible member to investigate the incident,
    iii. Action being undertaken by the Party to resolve the situation. This may include:
        1. Reports to the authorities,
        2. Banning the perpetrator from the Party's social media platforms and/or in-person events,
        3. Adding the perpetrator's information to a database that is tracked and updated to have supporting evidence for future instances;
        4. Any further actions, including timelines.

Should the complainant not receive a satisfactory response from the Provincial Council, they may appeal the decision within 30 days of receipt. The party should then assign the incident to a neutral third party to investigate the circumstances.

The complainant may choose to report the incident to legal authorities without affecting the Party's investigation.

B. **Perpetrator of technology-facilitated violence**

The Party will:

a. Make the process of reporting TFV perpetrated by one of its members publicly available;
b. Designate a member of the Provincial Council to receive and deal with complaints
    i. Should a member of the Provincial Council be directly linked to the case, they shall be temporarily removed from the Council until the incident is fully investigated.

The Investigator shall:

a. Interview the complainant and defendant separately and gain context for the incident;
b. Report back to the Provincial Council within 20 days of the original report being filed with updates including:
    i. Details of the incident;
    ii. Timelines for any action taken;
    iii. Recommended actions to resolve the situation including:
        1. Mandatory training,

2. Temporary suspension from the party,
3. Expulsion from the party,
4. Escalation to the authorities;

c. Provide the complainant with an update within 30 days to let them know the results of their complaint, including actions taken.

Should the complainant not receive a satisfactory response from the Provincial Council, they may appeal the decision within 30 days of receipt. The defendant may also appeal the decision within 30 days of receipt. In these two cases, the party should then assign the incident to a neutral third party for further investigation.

The complainant may choose to report the incident to legal authorities without affecting the Party's investigation.

6. Privacy

All those party to a TFV complaint are expected to respect the privacy and confidentiality of all other parties involved and to limit the discussion of a complaint to those that need to know.

7. Review

_____Party of Prince Edward Island will review this policy every 3 years, or as required, and will make necessary adjustments to ensure it meets the needs of all members.

8. Enquiries

Enquiries about this policy and related procedures may be made to _____.

Date: _____