

Catalysing Regional Action:

**A Toolkit for Parliamentarians on Addressing Technology-Facilitated
Gender-Based Violence (TFGBV)**

Table of Contents

Introduction.....	3
Legislative Planning to Address Technology-Facilitated Gender-Based Violence (TFGBV).....	5
Checklist for Legislative Planning to address TFGBV.....	8
<i>In your review of legislation.....</i>	8
<i>In your assessment of budgets.....</i>	9
<i>In your oversight role.....</i>	10
<i>In your constituency representation role.....</i>	10
<i>In cross-party collaboration and political processes.....</i>	11
<i>In monitoring emerging risks and future trends.....</i>	11
Code of Conduct for Digital Engagement.....	12
Sample Code of Conduct.....	17
1. Purpose and Scope.....	17
2. Core Principles for Digital Engagement.....	18
3. Rules of Conduct.....	18
4. Reporting, Investigation and Accountability Mechanisms.....	20
5. Monitoring, Review and Continuous Improvement.....	22
Community Engagement and Outreach Strategy to Raise Awareness on Technology-Facilitated Gender-Based Violence (TFGBV).....	23
<i>Outreach Planning Worksheet.....</i>	31
Guidance for Women in Public Life on Responding to Technology-Facilitated Gender-Based Violence (TFGBV) on Social Media.....	35

For more information on resources or technical assistance, contact the ParlAmericas International Secretariat at info@parlamericas.org



This toolkit was made possible by the generous support of the Government of Canada through Global Affairs Canada.

Published in July 2026

Introduction

Technology-facilitated gender-based violence (TFGBV) – recognized as a form of gender-based violence (GBV) and a violation of human rights, in accordance with international standards – is defined as “an act of violence committed, assisted, aggravated or amplified through information and communication technologies or digital media, against a person on the basis of their gender” (UNFPA, 2024).

Women in politics are disproportionately targeted due to harmful gender norms and stereotypes deeply rooted in Caribbean political and wider societal culture. Similar patterns of abuse are experienced by women journalists, activists, civil society leaders, human rights defenders and other women participating in public discourse. These acts of violence often focus on discrediting women’s credibility and leadership; policing their appearance, behaviour, or personal lives; silencing participation in public discourse; and reinforcing existing power imbalances and gender stereotypes.

This results in consequences that transcend the digital platforms and impacts various dimensions of one’s life and livelihood: stress, anxiety and impacts to one’s mental well-being and family-life, self-censorship and withdrawals from public, civic participation and digital spaces, as well as economic, career and reputational consequences. When women’s participation in public life is undermined by hostile digital environments, our societies suffer a loss of perspectives, we see declining interest among women in political and public life, and our democratic systems are weakened.

While women parliamentarians and political actors face heightened exposure due to their visibility, TFGBV is a harmful reality for women and girls writ large. This causes personal harm for victims, and has similar ripple effects across families and societies as a whole. In response to these complex issues, parliamentarians can play a crucial role in driving sustained efforts to address and prevent TFGBV through their parliamentary and political functions and platforms. This toolkit has been developed to support parliamentarians and political actors in this work by

Data on women’s lived experiences in the Caribbean reveals that this takes various forms: **online harassment and hate speech, cyberstalking and persistent digital monitoring, non-consensual sharing of intimate images or personal information (doxxing), impersonation or identity-based attacks, surveillance, coordinated disinformation and smear campaigns, and the use of shallow and deep fakes.**

providing guidance for legislative planning on TFGBV, a sample code of conduct for political parties and parliamentarians, community engagement, and outreach and awareness raising strategies. A tool also provides guidance for women in public life on responding to TFGBV on social media.

These tools were informed by the findings and inputs of women parliamentarians who participated in the regional study and a meeting on catalysing regional action on technology-facilitated gender-based violence in the Caribbean, undertaken through a collaboration between UNFPA, ECLAC, and ParlAmericas. The study amplified the voices and lived experiences of women leaders across the region and identified practical actions to strengthen prevention, protection, and response efforts for women in public life and for women and girls across the Caribbean more broadly.

Legislative Planning to Address Technology-Facilitated Gender-Based Violence (TFGBV)

There are significant legislative and policy gaps across the Caribbean in preventing and addressing technology-facilitated gender-based violence (TFGBV). These include, but are not limited to, the absence of clear legal definitions, limited public awareness, inadequate prevention and protection measures, insufficient survivor support services, weak evidence-gathering processes, inadequate training for law enforcement personnel, limited budgetary resources, insufficient regional legislative coordination, and challenges related to cross-border enforcement.

Adopting new and strengthening existing legislative frameworks on addressing TFGBV is crucial for reducing barriers to women's full and equal participation in public and political life, ending violence against women and girls in all forms and promoting inclusive societies and healthy and strong democracies for all.



Legislative Actions to Address TFGBV

Effective responses to TFGBV require a comprehensive legislative approach that incorporates prevention, protection, victim support, timely and effective responses, and enforcement mechanisms, while respecting fundamental rights such as freedom of expression and privacy. As TFGBV is seldom addressed through a single law in Caribbean jurisdictions and significant legislative and policy gaps remain, parliamentarians can consider the following strategies to strengthen legislative responses.

Consult Relevant Stakeholders and Constituents

Undertake broad consultations with constituents, subject-matter experts, women's rights organizations, survivors of TFGBV, youth organizations, media associations, digital rights advocates, information and communications technology companies, and other civil society and regional stakeholders. Meaningful consultation can help parliamentarians better understand the prevalence, scope, and social, cultural, political, health, and economic impacts of TFGBV on women and girls, as well as on other traditionally marginalized groups. It can also help identify emerging forms of digital violence and opportunities for legislative intervention.¹

¹ Understanding that there are differentiated and aggravated impacts on groups of women and girls historically subjected to [multiple forms of intersectional discrimination](#), including Indigenous, Afro-descendant, older women, young women, migrants, refugees, women with disabilities, rural and peasant women, as well as environmental and territorial women defenders, journalists, community leaders, human rights defenders, and digital activists, and

Review Existing Laws and Identify Legislative Gaps

Parliamentarians can review existing legislative and policy frameworks, including criminal laws, cybercrime and digital safety legislation, gender-based violence and domestic violence legislation, electoral laws, and relevant national policies and strategies, to assess the extent to which they address TFGBV.

This review should examine key elements such as definitions, offences, reporting mechanisms, provisions for prevention and protection, investigative powers, sanctions, and compensation for harm. It should also assess whether legislative provisions are clear, comprehensive, and capable of responding to evolving forms of digital violence while ensuring legal certainty and consistent interpretation.

The Inter-American Model Law to prevent, punish and eradicate gender-based digital violence (MESECVI) provides a baseline for comparative review of existing legislative frameworks and can guide decisions regarding legislative action, including amendments to existing laws, the repeal of outdated provisions, and the development of new legislation.

Build Consensus for Legislative Action

Successfully advancing legislative reform on TFGBV requires building support across Parliament. Parliamentarians can strengthen support for proposed measures by engaging colleagues within their caucus, sharing evidence and feedback gathered through consultations, highlighting the state's commitments under international and regional human rights frameworks, and fostering multi-party collaboration through mechanisms such as women's parliamentary caucuses.

Engaging parliamentary leadership, relevant committees, youth parliamentary bodies, and men as allies can further strengthen momentum and build broad ownership of reform efforts.

Key human rights frameworks on protecting women and girls against TFGBV

- The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)
- The Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women
- The International Labor Organization Convention No. 190 on Violence and Harassment
- Beijing Declaration and Platform for Action
- The United Nations General Assembly Resolution on Violence against Women and Girls Facilitated by Technology (2022)

underscoring that in many cases digital violence reproduces colonial, racist, and misogynistic stereotypes that seek to delegitimize their political and social leadership (MESECVI)

Ensure Adequate Resources for Implementation

Effective implementation of legislative measures to address TFGBV requires adequate financial and human resources. Parliamentarians can advocate for budget allocations that support prevention, timely response and investigation, protection measures, victim support services, and enforcement.

Resources may be required for specialized gender-sensitive training for first responders, law enforcement officers, prosecutors, judicial officers, and parliamentary staff; strengthening cybercrime units and related institutions; investing in technology and digital investigative tools; and supporting public education and awareness campaigns.

Funding should also be allocated to survivor-centred services, including psychosocial support, legal assistance, referral pathways, and digital safety services.

Monitoring the Implementation of Legislative Reforms

Parliamentarians play an important oversight role in monitoring the implementation and effectiveness of measures adopted to address TFGBV. Oversight activities may include reviewing implementation data, posing questions to ministers, conducting committee studies or inquiries, and examining reports from relevant government institutions.

Parliamentarians should also seek evidence from survivors, women's organizations, academic institutions, media associations, civil society organizations, and other stakeholders to better understand implementation challenges, identify gaps, and monitor emerging trends in digital violence.



Checklist for Legislative Planning to address TFGBV

The following checklist is designed to support parliamentarians and parliamentary staff in systematically addressing Technology-Facilitated Gender-Based Violence (TFGBV) through legislation, budgets, oversight, and constituency engagement. It adopts a technology-neutral and survivor-centered approach, focusing on conduct and harm rather than on specific platforms or tools, and recognizing the State's duty of due diligence to prevent, address, investigate, sanction, and remedy gender-based digital violence against women. It provides practical questions to help ensure legal and policy responses effectively prevent, address, and remedy online harms while protecting democratic participation and human rights.

In your review of legislation...

Objective: *To ensure laws adequately prevent, address, and sanction TFGBV while protecting freedom of expression, privacy, non-revictimization and democratic participation.*

- Does existing legislation explicitly address all forms of TFGBV such as – but not limited to – online harassment and hate speech, cyberstalking and persistent digital monitoring, non-consensual sharing of intimate images or personal information (doxxing), impersonation or identity-based attacks, surveillance, coordinated disinformation and smear campaigns and the use of shallow and deep fakes?
- Does the existing legislation provide adequate protection and justice for acts of digital violence that occur in private settings or public settings, whether the perpetrator(s) is known or unknown to the victim?
- Are legal definitions clear, technology-neutral, and adaptable to emerging digital harms?
- Do laws provide adequate protection for women in public and political life, and by extension all women and girls who are disproportionately targeted?
- Are reporting and complaint mechanisms accessible, confidential, survivor-centered with protection from revictimization, and safe to use with trauma-informed procedures?
- Are enforcement mechanisms realistic and implementable in digital environments?
- Do penalties appropriately reflect the seriousness of technology-facilitated gender-based violence, including aggravating circumstances and cumulative harm?
- Are safeguards included to protect freedom of expression and prevent misuse of legislation, including compliance with principles of legality, necessity, proportionality, and judicial oversight?
- Does legislation establish clear, enforceable obligations for digital platforms and service providers to prevent, respond to, and remedy TFGBV while protecting privacy and due process rights?

- Are procedures in place to enable timely protective measures, including harmful content removal or restriction, subject to judicial oversight, evidence preservation, and safeguards against censorship?
- Were women in politics, civil society groups, digital rights experts, and survivors consulted in developing or revising legislation, with particular attention to women facing intersecting forms of discrimination?
- Does the legislation recognize and address the disproportionate impacts of TFGBV on women experiencing intersecting forms of discrimination, including but not limited to women with disabilities, Indigenous women, and migrant women?
- Are review clauses included to allow updates as technology evolves?

In your assessment of budgets...

Objective: *To ensure sufficient resources exist to implement laws, support survivors, and prevent TFGBV sustainably.*

- Are resources allocated to law enforcement and judicial bodies to investigate and prosecute TFGBV cases?
- Is funding available for survivor support services, including legal aid and psychosocial assistance?
- Are public awareness and prevention campaigns funded adequately?
- Are resources allocated for public awareness, prevention and social norms change initiatives aimed at reducing the acceptance and normalization of TFGBV?
- Are digital literacy and safe online participation initiatives supported?
- Are institutions responsible for implementation adequately resourced and trained?
- Are investments made in technology and forensic tools needed to investigate online harms?
- Is funding available to support monitoring and research on TFGBV trends?
- Are resources allocated for public education campaigns on TFGBV, its impacts and the key dimensions of the legislation?
- Are sufficient resources provided to build partnerships with civil society organizations and community groups?

In your oversight role...

Objective: *To ensure government policies and programmes effectively prevent and respond to TFGBV and that accountability mechanisms function properly.*

- Are data collection systems tracking TFGBV incidents disaggregated by gender, age, context, and other relevant factors such as ethnicity, disability, migration status, and territorial location, in accordance with ethical and privacy safeguards?
- Are law enforcement agencies receiving appropriate gender-responsive training and resources?
- Are reporting and complaint mechanisms functioning efficiently and safely?
- Are survivors satisfied with access to justice, support services, and the responsiveness of institutions responsible for prevention and protection?
- Are regulatory or oversight bodies monitoring and holding platforms accountable for compliance with their obligations to prevent, address and remedy TFGBV?
- Are periodic reviews conducted on TFGBV legislation and implementation effectiveness?
- Are impact assessments conducted to evaluate the social and political effects of online violence?
- Is evidence from civil society and survivor experiences incorporated into oversight reviews?
- Are institutions publicly reporting progress and challenges transparently?

In your constituency representation role...

Objective: *To ensure communities understand TFGBV risks and that citizens' experiences inform legislative responses.*

- Are constituents aware of how TFGBV affects participation in public life and democracy?
- Are constituency offices equipped with information and referral pathways to support individuals experiencing TFGBV?
- Are women, youth, and marginalized groups consulted regarding their online safety concerns?
- Are mechanisms in place to receive community feedback about digital safety and harassment?
- Are local organizations and community leaders engaged in awareness and prevention efforts?
- Is information about reporting mechanisms and support services shared widely?
- Are constituency meetings and communications addressing safe online participation?
- Are experiences of women leaders and activists reflected in constituency advocacy?

In cross-party collaboration and political processes...

Objective: *To promote collective action to reduce TFGBV and protect democratic participation across political lines.*

- Are political parties encouraged to adopt codes of conduct for digital engagement?
- Are cross-party initiatives developed to address online violence, including responses to coordinated digital attacks during electoral periods?
- Are women's parliamentary caucuses or cross-party gender equality groups actively engaged in advancing legislative and policy responses to TFGBV?
- Are election-related digital harms being monitored and addressed?
- Are campaign environments promoting respectful digital discourse?
- Is cooperation encouraged to avoid politicization of online violence and discrimination issues?

In monitoring emerging risks and future trends...

Objective: *To ensure legislative responses remain effective as technology evolves.*

- Are emerging and evolving technologies being monitored for misuse in ways that may facilitate or amplify TFGBV, including but not limited to AI-generated content or deepfakes?
- Are regulatory and legislative frameworks flexible enough to address new digital harms?
- Are partnerships maintained with digital experts, technology companies, researchers, civil society organizations and regional institutions to monitor emerging trends and risks?
- Are early-warning or risk-monitoring mechanisms being developed?

Moving from Commitment to Action

Legislative reform alone cannot eliminate TFGBV. Effective responses require coordinated implementation, adequate resources, institutional accountability, prevention efforts, public education, and sustained collaboration among governments, parliaments, civil society organizations, technology actors, and communities. By championing legislative reform, promoting accountability, and exercising effective oversight, parliamentarians can help create an environment in which women participate fully, safely, and equally in public and political life, both online and offline.

Code of Conduct for Digital Engagement

Political Parties and/or Parliamentarians

Technology is an essential tool for political parties, parliamentarians, and electoral candidates, supporting their roles and responsibilities through its broad reach, speed, accessibility, and capacity to facilitate engagement with constituents. While it offers significant benefits for political, parliamentary, and electoral activities, it also exposes women and girls to disproportionate levels of technology-facilitated gender-based violence (TFGBV), undermining their ability to participate safely and equally in public and political life.

A code of conduct for digital engagement can play an important role in establishing standards of ethical behaviour and promoting respectful, safe, and responsible online engagement. It can also help strengthen democratic integrity, public trust, and inclusive political participation while protecting fundamental human rights. Recognizing the impact of online behaviour on democratic institutions and processes, this guide for developing a Code of Conduct is intended to support political parties, parliamentarians, and other relevant actors in developing or revising existing ethical frameworks and standards for digital engagement. It also provides resources and guidance to support the development of codes of conduct tailored to the specific needs and context of individual parliaments and political parties.

To ensure effectiveness, the development or revision of a code of conduct should involve consultation with key stakeholders and the meaningful participation of women. This can help ensure that the resulting framework is gender-responsive, culturally and politically relevant, and practical to implement.

Elements of a Code of Conduct for Digital Engagement

Purpose and Scope

A code of conduct for digital engagement by political parties and/or parliamentarians should seek to foster a culture of ethical, respectful, and responsible behaviour across digital and technological platforms. It should establish clear principles and standards of conduct, outline accessible, confidential, and survivor-centred mechanisms for reporting, referral, investigation, and complaints, and address the various forms of TFGBV and digital violence. A code of conduct should also promote public trust in political actors while protecting privacy and upholding fundamental human rights.

The purpose and scope of the code should be clearly defined. This section should also outline the institutional context in which the code applies, including the individuals and entities covered by its provisions.

Application Pathways for the Code of Conduct

A Code of Conduct for Digital Engagement may be adopted and applied in a variety of institutional contexts, including parliamentary institutions and political parties.

→ Parliamentary Adoption

Within parliamentary institutions, the Code may apply to elected and appointed parliamentarians, as well as parliamentary staff. It may be incorporated into existing standing orders, codes of conduct, ethics frameworks, workplace policies, or other institutional governance mechanisms. The scope of application should clearly identify the individuals covered by the Code, including members of parliament, senators, and parliamentary employees, regardless of employment status or contract type.

→ Political Party Adoption

Within political parties, the Code may apply to party leaders, executive members, candidates, elected representatives, party members, staff, volunteers, and campaign teams. It may be adopted through party constitutions, internal codes of conduct, membership agreements, campaign guidelines, or other governing instruments. The scope of application should clearly define the individuals and activities subject to the Code.

Core Principles and Ethical Standards

This section should establish the principles and ethical standards that guide the conduct of political parties, party members, parliamentarians, and electoral candidates on digital platforms, both within and outside parliamentary settings.

These principles may be informed by national legislation and relevant international and regional human rights instruments, including the [Universal Declaration of Human Rights](#), the [International Covenant on Civil and Political Rights](#), the [Convention on the Elimination of All Forms of Discrimination Against Women and Girls \(CEDAW\)](#), the [Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women \(Belem do Pará Convention\)](#) and the [UN General Assembly Resolution on the Elimination of Violence Against Women and Girls Facilitated by Technology](#).

In Practice:

In 2019, the British Virgin Islands outlined the following principles in their [Code of Conduct for Political Parties and Candidates](#) which can be used to protect persons from technology-facilitated gender-based violence:

- The emphasis must be on issues rather than personalities. Candidates must also avoid defamation of character of their opponents, their families and supporters.
- All political parties and their members and supporters, and all candidates and their supporters, must accept that others have the right to present their political principles and ideas in a peaceful environment without intimidation or fear of reprisal, and must respect that right.

Source: Office of the Supervisor of Election, British Virgin Islands

Several Latin American parliaments have adopted policies and institutional mechanisms to prevent and address gender-based violence in parliamentary workplaces, including technology-facilitated gender-based violence (TFGBV). Additional examples and good practices can be found in [Parliamentary Protocols on Gender-Based Violence](#) (available in Spanish) and the [ParlAmericas Parliamentary Practices for Gender Equality Dashboard](#).

Specific Rules of Conduct

This section should clearly define prohibited conduct and establish expectations for the online behaviour of parliamentarians, political parties, party members, and electoral candidates.

The code should clearly define the various forms of TFGBV and digital violence it covers, including online harassment and hate speech, cyberstalking and persistent digital monitoring, the non-consensual sharing of intimate images, doxxing, impersonation and identity-based attacks, digital surveillance, coordinated disinformation and smear campaigns, and the use of shallowfakes and deepfakes.

Example of rules of conduct

Political parties are encouraged to refrain from manipulative behaviour that threatens or has the potential to negatively impact values, procedures and political processes, in particular:

1. producing, using or disseminating falsified, fabricated, doxed or stolen data or material, including deep fakes generated by artificial intelligence systems;
2. producing, using or disseminating misleading or hateful content; and

3. using manipulative tactics, techniques and procedures to disseminate or amplify political messages.

Source: [*Commission Recommendation \(EU\) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament*](#)

Investigation and Accountability Mechanisms

This section should identify the individual(s), office(s), or body responsible for receiving, processing, and investigating complaints. It should also outline procedures for reporting, investigation, decision-making, appeals, and the enforcement of sanctions or disciplinary measures for breaches of the code.

Recognizing the significant harm that digital violence can cause, institutions may wish to establish expedited procedures for addressing serious violations, including the temporary or permanent removal or restriction of online content where appropriate. Such procedures should ensure that relevant evidence is preserved for investigative and disciplinary purposes.

To protect complainants and witnesses, clear standards on confidentiality, privacy, and non-revictimization should be established for all individuals involved in receiving, investigating, and adjudicating complaints.

Given varying institutional capacities, different models may be used to administer complaints and accountability processes. Options include:

- An internal ethics, standards, or disciplinary committee (such as a parliamentary ethics committee or party disciplinary body);
- A designated ombudsperson or focal point responsible for digital conduct and harassment issues;
- An existing human resources, compliance, or integrity office, where appropriate;
- Relevant law enforcement agencies, cybercrime units, gender-based violence units, electoral authorities, or judicial bodies where criminal or regulatory violations are alleged; or
- A hybrid model in which complaints are initially received through a centralized mechanism and referred to the appropriate authority based on the nature and severity of the alleged violation.

Roles, mandates, and referral procedures should be clearly defined to avoid gaps, duplication, and conflicts of interest.

Examples of Investigation and accountability mechanisms

In Canada, only cases that meet a 'Threshold Test and Standard' are investigated. This threshold is determined by a policy which states, 'whether there exist reasonable grounds to believe that the gravity or seriousness of the alleged offence would justify committing investigative resources' along with consideration of 'public interest factors.'

Source: *Special Investigators mechanisms*, Elections Canada

On the basis of managing evidence to support investigations, these good practices are adapted from the [ACE Project Electoral Knowledge Network](#), which include:

- Labelling evidence by assigning a specific reference number for each piece of evidence. The personnel responsible for collecting the evidence should record where the evidence was taken into custody and when (date and time). This recording should be kept on file, and a duplicate copy of the recording should be given to the person who originally provided the evidence, and a copy is kept in the file;
- Original documents, media files, hyperlinks, screenshots and evidence should be sealed, protected in documents and placed into evidence in boxes, containers or password protected databases and only using photocopies or digital copies for the investigation; and
- Keeping the records dealing with the handling of evidence separate from the complaint file.

Monitoring and Periodic Review

Political parties and parliamentary institutions should establish mechanisms to periodically review the implementation and effectiveness of the code of conduct. Such reviews may assess emerging digital risks, analyze trends in complaints and outcomes, evaluate compliance with the code, and identify areas requiring additional training, policy reform, or institutional support.

Regular review helps ensure that the code remains relevant, responsive to technological developments, and effective in addressing emerging forms of TFGBV and digital violence.



Sample Code of Conduct

The following Sample Code of Conduct provides a practical framework to assist parliamentarians and political parties in developing or strengthening measures to address Technology-Facilitated Gender-Based Violence (TFGBV). It includes sample provisions, procedures, and standards that may be adapted to support prevention, reporting, investigation, accountability, and redress, while promoting safe digital engagement and protecting democratic participation and human rights.

1. Purpose and Scope

Purpose:

The purpose of this Code of Conduct is to:

1. Promote respectful, safe, and responsible digital conduct and engagement by parliamentarians and political parties in order to protect and uphold democratic integrity, fundamental human rights, public trust, inclusive political participation and gender equality;
2. Foster a common understanding of the prevalence and impacts of Technology-Facilitated Gender-Based Violence (TFGBV) on individuals in public and political life, particularly women;
3. Define unacceptable forms of conduct and behaviour;
4. Establish the key principles and ethical standards that guide the conduct of parliamentarians, political parties, and their members in digital spaces; and
5. Set out procedures and mechanisms for reporting, investigating and addressing violations of this Code.

Scope and Application:

This Code applies to all elected and appointed parliamentarians, political parties, and, where applicable, their members, staff, volunteers, contractors, and representatives in relation to digital engagement undertaken in the course of political, parliamentary, electoral, or public activities.

This Code applies to conduct occurring on social media platforms, messaging applications, websites, email communications, digital campaign tools, artificial intelligence-enabled systems, and any other digital or technology-enabled platforms.

Responsibility for the administration and enforcement of this Code shall rest with [insert relevant body, such as the electoral commission, parliamentary standards commissioner, ethics body, or another designated independent authority, as appropriate within the national context].

The designated authority may receive complaints, conduct investigations, determine whether breaches of the Code have occurred, and recommend or impose sanctions in accordance with established procedures.

Nothing in this Code limits the reporting of conduct that may constitute a criminal offence to the appropriate law enforcement or judicial authorities.

2. Core Principles for Digital Engagement

This Code is informed by applicable national legislation, international human rights commitments, and the Inter-American Model Law to Prevent, Punish and Eradicate Gender-Based Violence Against Women.

These frameworks recognize the rights to life, privacy, autonomy, equality, freedom of expression, political participation, and a life free from violence. The following principles shall guide conduct under this Code:

- Respect and dignity;
- Gender equality and non-discrimination;
- Intersectionality;
- Responsible political debate and engagement;
- Due diligence, transparency and accountability;
- Protection of democratic participation;
- Commitment to non-violent communication;
- Survivor-centered approaches, confidentiality, and non-revictimization;
- Security and protection grounded in a human-rights approach; and
- Access to justice and accountability.

3. Rules of Conduct²

Parliamentarians, political parties, and their representatives **shall not engage in** any of the following conduct:

1. Access another person's digital accounts without authorization or impersonate an individual through digital platforms for the purpose of obtaining personal information, causing harm, or misleading others regarding that person's identity;
2. Possess, store, distribute, publish, or threaten to distribute private messages, images, photographs, videos, or audio recordings of an intimate or sexual nature without the

² These rules are inspired and informed by Articles 7 and 8 of the [Inter-American Model Law to Prevent, Punish and Eradicate Gender- Based Violence against Women, on Manifestations of Gender-Based Digital Violence Against Women](#).

individual's consent, whether such content is real, altered, or generated through digital technologies;

3. Harass, stalk, monitor, intimidate, or surveil an individual through digital technologies, devices, products, or services in an unwanted, repeated, or persistent manner;
4. Deploy spyware, tracking tools, surveillance technologies, or recording devices without lawful authority or consent for the purpose of monitoring, intimidating, or violating an individual's privacy;
5. Produce, distribute or circulate any content that violates a person's right to privacy and control over personal information;
6. Harass, intimidate, demean, threaten, or defame any individual through messages, comments, calls, coordinated postings, images, videos, or other digital content, particularly where such conduct is motivated by gender or other protected characteristics;
7. Create, distribute, or promote knowingly false, manipulated, or malicious content intended to harm an individual's reputation, safety, participation, or integrity;
8. Create, disseminate, support, or facilitate coordinated campaigns that seek to silence, intimidate, discredit, harass, demean, dehumanize, or exclude women or other traditionally marginalized groups from political or public life;
9. Publish, share, or promote content that incites violence, discrimination, hatred, or unlawful acts against an individual or group on the basis of gender, gender identity or expression, age, sexual orientation, race, ethnicity, religion, disability, physical appearance, geographic location, or any other protected characteristic;
10. Use digital communications to threaten, intimidate, coerce, or harass individuals, their families, or their associates for the purpose or effect of discouraging, limiting, or preventing their participation in political or public life;
11. Engage in or facilitate coordinated disinformation campaigns that intentionally undermine the participation, credibility, safety, legitimacy, or electoral prospects of women and other historically marginalized groups;
12. Use artificial intelligence systems or other digital technologies in a manner that contributes to discrimination, harassment, manipulation, deception, or technology-facilitated gender-based violence;
13. Create or knowingly disseminate artificially generated or manipulated content for the purpose of deceiving, defaming, harassing, intimidating, or suppressing democratic participation;
14. Obstruct, interfere with, or retaliate against any person involved in reporting, investigating, or adjudicating an alleged violation of this Code.

Prevention and Support Measures

Political parties and parliamentary institutions are encouraged to:

- Conduct regular training on digital ethics, online safety, TFGBV, responsible use of digital technologies, and reporting mechanisms;
- Promote awareness of this Code and related procedures among members, staff, and volunteers;
- Establish digital safety protocols and risk mitigation measures; and
- Encourage respectful and inclusive digital engagement.

Political parties and parliamentary institutions should also seek to provide survivor-centred support measures, including:

- Psychological support, counseling and mental health services;
- Legal information and legal aid services;
- Referral pathways to specialised gender-based violence services;
- Timely and survivor-centered responses;
- Assistance with content reporting and removal where appropriate;
- Public statements of support where appropriate; and
- Education and training on digital safety and reporting mechanisms.

4. Reporting, Investigation and Accountability Mechanisms³

The following provisions provide guidance for reporting, investigation, and accountability processes.

Reporting Complaints

1. Any parliamentarian, political candidate, party member, staff member, volunteer, contractor, or other person authorized under this Code may submit a complaint regarding an alleged breach of the Code.
2. Complaints may be submitted in writing or verbally to the designated authority responsible for receiving and investigating complaints. Where possible, relevant evidence should accompany the complaint.
3. Mechanisms for receiving complaints should be accessible, confidential, survivor-centred, and responsive to the needs of diverse users.

³ These recommended guidelines for reporting, investigation and accountability are informed and inspired by the [Standards for Codes of Conduct for Members of Parliament and the Parliamentary Workplace](#), Commonwealth Parliamentary Association and adopts a hybrid approach to investigations.

Investigating Procedures

1. Personnel responsible for receiving and investigating complaints shall act fairly, impartially, and independently, and shall adhere to principles of confidentiality, procedural fairness, and survivor-centred practice.
2. Investigators should possess appropriate expertise in digital conduct, technology-facilitated violence, investigative procedures, and the protection of sensitive information.
3. The complainant, respondent, and witnesses shall cooperate in good faith with any investigation conducted under this Code.
4. Appropriate measures shall be established to protect complainants and witnesses from retaliation, intimidation, harassment, or further harm.
5. Respondents shall be informed of the allegations against them, provided with relevant evidence, and granted a reasonable opportunity to respond.
6. Investigations should be completed within timelines established by the designated authority and communicated to the parties involved.
7. Where alleged conduct may constitute a criminal offence, the matter should be referred promptly to the appropriate law enforcement, cybercrime, electoral, or judicial authority.

Sanctions and Corrective Measures

1. Where a breach of the Code is established, sanctions should be proportionate to the severity, intent, impact, and recurrence of the misconduct, while ensuring due process and procedural fairness.

Possible sanctions may include:

- Written warnings;
 - Removal of offending content,
 - Public apologies or corrective statements;
 - Mandatory education or training;
 - Temporary suspension of privileges or responsibilities;
 - disciplinary measures imposed by the relevant political party or parliamentary body;
 - Exclusion from specific activities or leadership positions;
 - Disqualification from office or candidature, where legally permissible; and
 - Referral for civil, regulatory, or criminal proceedings where appropriate.
2. Where appropriate and consistent with privacy considerations, findings and outcomes may be published to promote transparency, accountability and public confidence.

5. Monitoring, Review and Continuous Improvement

Political parties and parliamentary institutions should establish mechanisms to periodically review the implementation and effectiveness of this Code.

Such reviews may:

- assess emerging digital risks and technological developments;
- monitor complaints, investigations, outcomes, and trends;
- evaluate compliance with the Code;
- identify areas requiring additional training, policy reform, or institutional support; and
- assess whether the Code continues to effectively address emerging forms of TFGBV and digital violence.

The Code should be reviewed at regular intervals and updated as necessary to reflect evolving technologies, societal developments, legal frameworks, and best practices in the prevention of technology-facilitated gender-based violence.

Guidance for the Development of Codes of Conduct

[UK Committee on Standards in Public Life \(CSPL\): Review of Political Parties' Codes of Conduct, 2019](#): The frameworks included provisions on respectful behaviour, anti-harassment, and non-discrimination, with explicit expectations for members' conduct in online spaces. While not always framed as standalone digital engagement codes, they demonstrate how political parties operationalize standards for behaviour across both offline and digital environments, offering practical language and enforceable structures that can inform the development of more tailored guidance.

[Codes of Conduct on the Rise: Fair and Ethical Political Campaigning Online, International IDEA, 2024](#): A relevant reference point developed by International IDEA on ethical online campaigning, which addresses key issues such as disinformation, transparency, and the role of digital platforms in shaping political discourse. This work emphasizes the value of co-created, voluntary codes of conduct that are developed collaboratively among political actors, helping to build shared ownership and increase compliance. It also highlights the importance of aligning digital engagement standards with broader democratic principles, offering a useful normative framework for shaping clear, credible, and context-sensitive approaches to online political behaviour.

Community Engagement and Outreach Strategy to Raise Awareness on Technology-Facilitated Gender-Based Violence (TFGBV)

While legislative reform, institutional policies, and accountability mechanisms are critical for addressing technology-facilitated gender-based violence (TFGBV), they must be complemented by broader efforts to engage communities, raise awareness, strengthen partnerships, and promote positive social norm change. Persistent gender stereotypes, discriminatory social norms, limited awareness, and the normalization of harmful online behaviours continue to create conditions that enable TFGBV and undermine the full and equal participation of women in public and political life.

Community engagement, public education, advocacy, and multi-stakeholder collaboration are essential for preventing TFGBV, challenging harmful attitudes and behaviours, and fostering safer and more inclusive digital spaces. Parliamentarians are uniquely positioned to convene stakeholders, amplify public awareness, gather evidence and community perspectives, and champion initiatives that promote safe and equitable participation in public and political life.

This section provides parliamentarians, women's parliamentary caucuses, and other relevant actors with practical strategies, resources, examples, and good practices for engaging communities, informing policy and decision-making, and advancing efforts to prevent and address TFGBV.

Engaging the Community: A Key Component of Ending TFGBV

As trusted community leaders, parliamentarians can help increase understanding of TFGBV, amplify the experiences of those affected, and support efforts to prevent violence before it occurs. Community engagement also enables parliamentarians and political actors to better understand how TFGBV affects their constituents, identify emerging trends and challenges, and recognize gaps in protection, support services, and public awareness.

Effective outreach can:

- Increase public understanding of TFGBV and its impacts;
- Challenge harmful gender stereotypes and discriminatory norms;
- Promote respectful digital engagement;
- Encourage reporting and support-seeking, and increase awareness of available support services and referral pathways;
- Reduce stigma around victims and survivors;

- Strengthen digital literacy and critical thinking skills; and
- Strengthen democratic participation, particularly among women and marginalized groups.

Prevention efforts are most effective when they engage entire communities, including women and girls, men and boys, educators, media professionals, civil society organizations, technology actors, and public institutions. Sustainable change requires collective ownership of the issue and coordinated action across multiple sectors.

Identifying Strategies for Outreach and Engagement

The most appropriate outreach and engagement strategy will depend on the intended objectives. These may include gathering perspectives, lived experiences, and evidence to inform policy, legislation, and decision-making; raising awareness of the prevalence and impacts of TFGBV; promoting positive social norm change; or educating constituents about prevention measures, reporting mechanisms, and available support services.

The following are examples of outreach and engagement approaches that parliamentarians and other stakeholders may use to raise awareness of TFGBV and promote safer and more inclusive digital spaces.

Online Surveys

Parliamentarians and parliamentary committees can use online surveys to gather information on public awareness, perceptions, experiences, and knowledge related to TFGBV. Surveys can be an effective tool for identifying gaps in awareness, understanding community needs and concerns, and informing legislative, policy, advocacy, and outreach initiatives.

Where surveys are used, consideration should be given to confidentiality, informed consent, data protection, and the safety of participants, particularly when collecting information related to experiences of violence. Questions should be designed to minimize the risk of harm or re-traumatization and include information on available support services where appropriate.

Example:

The Joint Select Committee on Human Rights, Equality and Diversity launched an [online survey](#) to support its inquiry into the effects of period poverty in Trinidad and Tobago. The Committee promoted the survey through sponsored social media advertisements to broaden public participation and collect community perspectives. This provides an example of how digital engagement tools can be used to raise awareness, gather evidence, and better understand the experiences of those affected by issues such as TFGBV.

Constituency Offices

A constituency office can serve as an important avenue for raising awareness of TFGBV and engaging directly with constituents. In many cases, constituency offices are more accessible to the public than a country's parliament and often serve as the primary point of contact for information, services, and assistance. As a result, constituency offices can be used to support a range of outreach and engagement activities, including:

- Coordinating public workshops on digital safety, responsible digital engagement, and acceptable and unacceptable online behavior;
- Organizing meetings involving parliamentarians, law enforcement agencies, judicial officials, women's organizations, and community groups to develop awareness-raising initiatives;
- Providing constituents with information on relevant legislation, policies, and legal avenues for addressing TFGBV;
- Disseminating information on available support services and referral pathways for individuals experiencing TFGBV; and
- Assisting constituents through casework and referrals to appropriate authorities and support services where incidents of TFGBV are identified.

Community Initiatives

Parliamentarians can partner with civil society organizations, women's and youth organizations, educational institutions, and other community stakeholders to implement initiatives that raise awareness of TFGBV. These initiatives may include workshops in schools and universities, the distribution of informational materials such as flyers and posters, community education campaigns, intergenerational dialogues, the engagement of faith-based and community leaders as advocates, and digital safety programmes for women and girls.

Town Hall Meetings

Town hall meetings can be an effective means of consulting constituents and gathering perspectives on TFGBV. They provide opportunities to engage women, men, girls, and boys in discussions about their experiences, concerns, and recommendations related to technology-facilitated gender-based violence. Town hall meetings can also serve as forums for raising awareness of the various forms, impacts, and consequences of TFGBV and for sharing information on available support services and reporting mechanisms.

Special consideration should be given to creating safe, inclusive, and accessible spaces that enable women, young people, and traditionally marginalized groups to participate meaningfully and share their experiences without fear of stigma, retaliation, or further harm.

Example:

Parish Speaks, a periodically-held town-hall meeting styled opportunity for citizens to interact with the Government of Barbados. Prime Minister Mia Mottley, Government Ministers and senior officials of government ministries and departments visit each Parish to hear the concerns of the constituents and create solutions.

National Action Plan

A National Action Plan on TFGBV can serve as an important mechanism for coordinating and advancing a comprehensive response to the issue. Such a plan can establish priority actions, provide an evidence-based assessment of the prevalence and impacts of TFGBV, set clear objectives and targets, identify responsible institutions, outline resource requirements, and incorporate monitoring and evaluation mechanisms to measure progress and accountability.

Parliamentarians and relevant government ministers can play an important role in advocating for the development, implementation, and regular review of a National Action Plan on TFGBV. To ensure a coordinated and effective response, the development of the Plan should involve consultation and collaboration with key stakeholders, including law enforcement agencies, judicial authorities, women's parliamentary caucuses, gender equality institutions, cybercrime units, educational institutions, civil society and non-governmental organizations, parent-teacher associations, media organizations, technology companies and platforms, survivors, and other relevant stakeholders.

A National Action Plan on TFGBV should be grounded in a human rights-based and intersectional approach and include clearly defined institutional responsibilities, budgetary allocations, implementation timelines, and monitoring and evaluation frameworks. Where possible, it should align with relevant international and regional commitments and standards.

Media Campaigns

Media can be a powerful tool for raising awareness of TFGBV, promoting gender equality, and amplifying key advocacy messages. Parliamentarians and parliamentary institutions can use media campaigns to educate the public about the prevalence and impacts of TFGBV, build support for legislative and policy reforms, and increase awareness of available reporting mechanisms and support services. Outreach efforts may include the use of social media platforms, newspapers, television, radio broadcasts, and community public address systems to reach diverse audiences.

Media campaigns should employ survivor-centred, gender-responsive, and human rights-based messaging that avoids victim-blaming, challenges harmful stereotypes, and promotes accountability for perpetrators and institutions.

Example:

In 2025, the [UNFPA Caribbean](#) created an online campaign on digital violence in light of the 16 Days of Activism. Numerous organisations and individuals shared campaign content across social media platforms using #16Days #UNiTE #EndDigitalViolence #CaribbeanAgainstGBV

Political Party Conventions and Meeting

Political party conventions, annual meetings, and other party gatherings provide valuable opportunities to engage members on social issues such as TFGBV. Given the broad reach of political parties and their role in shaping political culture and public discourse, these forums can be used to raise awareness of TFGBV, facilitate dialogue on respectful online engagement, and gather feedback from members on challenges and potential solutions.

Political parties may also use these occasions to promote internal policies, codes of conduct, and educational initiatives aimed at preventing TFGBV and fostering respectful, safe, and inclusive digital engagement among members, supporters, candidates, and elected representatives.

Identifying Priority Groups for Engagement

Different groups experience TFGBV in different ways and may require tailored outreach and engagement approaches. Awareness-raising, education, and advocacy initiatives are often most effective when designed with the needs, experiences, and circumstances of specific audiences in mind.

The following groups may be considered priority audiences for engagement. For each group, examples of outreach activities, key messaging considerations, and engagement objectives are provided to support targeted and effective interventions.

Group	Focus of Outreach	Example of Activities	Example of Messaging
Women and Girls	Recognizing TFGBV and unsafe online behavior Digital safety and self-protection strategies	Workshops on digital safety and positive social media usage	<i>"Everyone has the right to participate online without fear."</i>

	Available reporting mechanisms and support services – and the importance of reporting Encouraging participation in public life	Dialogues with women’s organizations School or university sessions	<i>"Online abuse is real harm and support is available."</i> <i>"Online GBV violates human rights and must not be tolerated."</i> <i>"Digital spaces should be safe, inclusive and free from violence."</i> <i>"Your voice matters online and offline."</i>
Youth and Students	Responsible digital citizenship Recognizing harmful online behavior Bystander intervention Respectful political engagement online	School presentation on positive social media usage Youth-led campaigns on digital safety Social media challenges	<i>"Think before you post."</i> <i>"Respect online is respect in real life."</i> <i>"Check the data before making it viral."</i>
Men and Boys	Challenging harmful norms and behaviors Encouraging allyship Promoting respectful online interaction	Community dialogues Sports or youth club discussions Peer education initiatives	<i>"Respect online starts with you."</i> <i>"Strong communities stand against online abuse."</i> <i>"Online GBV is an issue for all. Being an ally means taking action."</i> <i>"Leadership includes promoting respect online."</i>

Political Actors and Party Supporters	Responsible digital engagement Understanding TFGBV in political spaces Promoting respectful campaign environments	Party workshops Campaign briefings Candidate training sessions	<i>"Strong democracy requires respectful debate."</i> <i>"Disagreement does not justify abuse."</i> <i>"Political competition should never justify violence or abuse."</i>
Media and Influencers	Understanding TFGBV, ethical reporting and digital security Responsible reporting on online abuse Avoiding amplification of harmful content Promoting accurate information	Media briefings Journalist training sessions Partnerships with influencers	<i>"Accurate reporting protects democratic participation."</i> <i>"Online abuse causes real harm – silence enables it."</i>

Monitoring Impact

Monitoring and evaluation are important components of effective outreach and engagement initiatives. Parliamentarians and other stakeholders should assess the extent to which activities contribute to increased awareness, improved knowledge, shifts in attitudes and behaviours, and greater uptake of reporting mechanisms and support services. Participant feedback and other relevant data can help inform future initiatives, strengthen outreach strategies, and ensure that efforts remain responsive to community needs and emerging forms of TFGBV.

Good practices for sensitization and countering disinformation and misinformation

TFGBV is often accompanied by misinformation and coordinated online narratives that target women and other traditionally marginalized voices, reinforcing discrimination and violence.

Common misinformation narratives may include:

- Assertions that online abuse is “not real violence” and has no real consequences;
- Blaming victims for online attacks and abuse they experience;
- Framing TFGBV protections as censorship or attacks on freedom of expression; and
- Minimizing or denying gendered harms.

Sensitization efforts may include:

- Providing clear, factual and rights-based information about TFGBV;
- Actively addressing and debunking common myths and harmful narratives;
- Promoting digital literacy;
- Encouraging verification of information before sharing;
- Using trusted data and evidence from credible sources;
- Equipping participants with skills to identify manipulated images, deepfakes and coordinated disinformation campaigns; and
- Promoting media literacy and critical consumption of online information.

Outreach Planning Worksheet

The following worksheet is designed to support parliamentarians, parliamentary staff, and partners in translating principles into action. It can be used to design a single activity or to structure a broader outreach initiative, ensuring that objectives, audiences, messaging, partnerships, and evaluation measures are clearly defined from the outset.

1. Define the Objective

What do you want this outreach activity to achieve?

- Increase awareness of TFGBV
- Promote respectful online behavior
- Inform people about reporting mechanisms
- Obtain data on person's lived experiences and the impacts
- Challenge harmful gender stereotypes and social norms
- Promote digital literacy and online safety
- Strengthen awareness of support services
- Support women's political participation
- Gather community input
- Other: _____

Specific objective:

2. Identify the Target Group

Primary audience:

Secondary audience (if any):

Why is this group important to reach?

3. Key Messages

Main message:

Supporting messages:

How will messages be adapted to this group?

4. Outreach Activities

Type of activity:

- Workshop
- Community meeting
- School session
- Social media campaign
- Media engagement
- Training session
- Other: _____

Description of activity:

Estimated number of participants:

5. Partners and Stakeholders

Organizations or groups to involve:

Community leaders or trusted focal points:

6. Communication Channels

How will participants be reached?

- Email
 - Social media/WhatsApp
 - Traditional mass media (Radio, TV, print media)
 - Schools
 - Community organizations
 - Mobile public announcement systems
 - Other:
-

7. Addressing Misinformation

Potential misinformation risks:

What steps can be taken to prevent misinformation and, how can it be addressed if it happens?

8. Logistics

Date:

Location:

Resources needed:

9. Monitoring, Evaluation and Reflection

How will you know if the activity was successful?

- Attendance
- Participant feedback
- Knowledge gained

- Engagement levels
- Follow-up requests
- Other: _____

Lessons learned:

10. Follow-up Actions

As a result of this initiative, what policy, legislative, oversight, advocacy or constituency actions will you undertake to address TFGBV, based on community needs?

Next steps:

Guidance for Women in Public Life on Responding to Technology-Facilitated Gender-Based Violence (TFGBV) on Social Media

Despite ongoing efforts to strengthen legislative frameworks, institutional safeguards, and public awareness, women in public and political life continue to experience online abuse, harassment, intimidation, and other forms of digital violence. As a result, many are required to make decisions about how to navigate and respond to these experiences in real time.

While responsibility for addressing TFGBV should never rest solely with those who experience it, practical guidance can help women in public life make informed decisions about their safety, well-being, and participation in digital spaces. The objective of this guidance is to support informed decision-making, reinforce personal agency, and contribute to safer and more inclusive digital environments, while recognizing that sustainable responses to TFGBV require coordinated action by states, legislatures, political parties, institutions, technology platforms, and society as a whole.

It is important to recognize that there is no single or universally correct way to respond to TFGBV. Responses will vary depending on the nature of the harm, individual circumstances, available support systems, and personal preferences. This section provides practical considerations and response options to support women in navigating and addressing TFGBV while maintaining agency over their participation in digital spaces.

Preparing for Potential Incidents⁴

Planning ahead can support more consistent, intentional responses and reduce the need for reactive decision-making.

- Define Parameters for Engagement
 - Identify which types of interactions warrant engagement or a response;
 - Clarify thresholds for blocking, reporting, or escalation; and
 - Determine the tone and approach you wish to maintain in public communications.
- Anticipate Areas of Risk
 - Consider issues or topics that may generate heightened visibility, engagement or backlash; and

⁴ The strategies outlined below are intended to support personal agency and informed decision-making. They do **not** replace the responsibility of perpetrators, institutions, platforms, or the State to prevent and respond to technology-facilitated gender-based violence.

- Recognize that abuse may arise unpredictably and is not always linked to controversial content.
- Prepare in Advance
 - Develop a personal digital safety plan, including emergency contacts, reporting pathways and support networks;
 - Develop response templates for recurring types of comments, abuse, or misinformation;
 - Establish moderation practices, individually or with a trusted team where applicable;
 - Identify a trusted colleague or advisor who can provide perspective before responding in complex situations; and
 - Familiarize yourself with available institutional, legal, and platform-specific reporting mechanisms.
- Strengthen Digital Security
 - Use strong passwords and multi-factor authentication;
 - Regularly review privacy and security settings;
 - Limit the sharing of sensitive personal information;
 - Conduct periodic searches of your public online presence to identify potential misuse of images, personal information or impersonation accounts; and
 - Consider separating personal and professional accounts where appropriate.

Responding to Incidents of Abuse

A structured approach can support measured and effective responses.

Apply a Decision-Making Framework

Before engaging, consider:

- Whether the interaction is constructive or intended to provoke;
- The potential impact of responding, including whether it may amplify harmful content;
- Whether the content may violate platform policies, institutional codes of conduct, electoral regulations, workplace policies, or criminal law; and
- Whether engagement aligns with your broader communication objectives.

Response Options

- **Do not engage:** In many cases, non-response is the most effective approach.
- **Respond selectively:** Where clarification or public accountability is warranted.
- **Restrict or block:** To maintain a safe and manageable online environment.

- **Report content:** Using platform mechanisms where policies are violated.
- **Seek support or escalate:** Particularly in cases involving coordinated attacks, threats to safety, image-based abuse, stalking, impersonation, doxxing or persistent harassment.

Managing Escalation

In situations involving increased visibility or coordinated activity:

- Take time to assess before responding;
- Prioritize personal safety and well-being when assessing whether and how to engage;
- Coordinate messaging with trusted advisors or team members;
- Maintain consistency in tone and messaging;
- Consider temporarily limiting comments or restricting account interactions where platform tools allow; and
- Avoid engaging in reactive exchanges that may escalate the situation.

Document, Report, and Escalate Where Appropriate

Systematic documentation can support accountability and appropriate follow-up.

- Document Incidents
 - Capture screenshots, including timestamps and account details;
 - Save links and maintain records of repeated or coordinated behaviour; and
 - Keep records securely and consider backing up evidence in a protected location or with a trusted individual.
- Use Reporting Mechanisms
 - Report content using platform reporting tools; and
 - Where relevant, use institutional or organizational channels, including parliamentary ethics bodies, political party mechanisms, professional associations, workplace grievance systems or media regulatory bodies.
- Escalate When Necessary

Where available and appropriate, women experiencing TFGBV may also consider engaging formal complaint mechanisms, electoral authorities, ombudspersons, judicial channels, or law enforcement agencies. Institutions have an obligation to provide accessible, safe, confidential, and survivor-centred responses, including protective measures where digital violence threatens an individual's integrity, safety, or participation in public life.

Particular consideration should be given to escalating incidents involving:

- Threats of violence;
- Persistent, targeted, or coordinated harassment;
- Stalking, impersonation, or image-based abuse; or
- The exposure of personal or sensitive information.

Considerations for Mental Health and Well-being

Experiences of TFGBV can have cumulative emotional and psychological effects.

- Take breaks from online engagement where needed;
- Seek support from trusted peers, networks, support services, or mental health professionals. Seeking support is a sign of strength and may be essential to maintaining long-term participation in public life;
- Recognize that these attacks are often the result of broader patterns of gender-based violence and should not be understood as reflective of individual merit, ability, or actions; and
- Recognize that, when directed at women in public and political life, such acts may constitute political gender-based violence and may undermine democratic participation, freedom of expression, equality, and meaningful participation in decision-making.

Maintaining well-being is an important component of sustained participation in public life.

Advocacy, Solidarity, and Collective Action

Addressing TFGBV requires collective approaches that extend beyond individual responses.

- Promote Positive and Respectful Engagement
 - Use platforms to model constructive and respectful discourse; and
 - Share accurate and evidence-based information to counter misinformation and disinformation.
- Support Other Women in Public Life
 - Express solidarity with those experiencing abuse;
 - Contribute to a culture where such behaviour is not normalized, tolerated, or ignored; and
 - Promote survivor-centred responses and accountability for perpetrators.
- Strengthen Alliances
 - Engage across political lines where appropriate;
 - Collaborate with civil society organizations, media organizations, professional associations, technology platforms and advocacy groups; and

- Encourage active allyship, including from male colleagues and other influential voices.

Know Your Rights

All women - including those experiencing TFGBV - have the right to:

- Live free from violence and discrimination;
- Participate fully in public, political and civic life;
- Access justice and effective remedies;
- Seek support and protection without fear of retaliation; and
- Enjoy freedom of expression while maintaining personal safety, dignity and well-being.