UK Parliament

COMMONWEALTH PARLIAMENTARY ASSOCIATION UK

MARCH 2022

A GUIDE TO MANAGING ONLINE & OFFLINE ABUSE

INTRODUCTION

Across the Commonwealth, democracy has gone digital. From the use of Twitter accounts by UK MPs to WhatsApp groups for constituents in Sierra Leone, social media platforms are now a vital aid to parliamentarians carrying out their duties.

Such use of technology has allowed representatives to easily communicate their work and provided constituents the opportunity to voice their concerns directly. This was particularly true during the Covid-19 pandemic where parliamentarians could no longer hold surgeries under social distancing rules. This unrestricted access through social media has, however, led to a surge in online abuse and harassment, largely targeted at women in politics. Such violence is both gender-based and political, used to reinforce gender inequality and deter women from being, or becoming, politically active.

An Inter-Parliamentary Union (IPU) study into harassment of women parliamentarians found that 42% of women MPs interviewed globally said they had been a target of abusive, sexual or violent content and behaviour on social media. CPA UK research has found that women parliamentarians have received abuse online in the form of abusive and discriminatory language, as well as threats of physical or sexual violence. In many cases, CPA UK found that these experiences have changed how parliamentarians communicate online, with many women MPs either reducing or no longer using a particular platform. Online abuse is silencing the important voices of women representatives in our democracies.

The existence of this modern form of violence against women in politics must be understood as a continuum of offline violence, and not a separate phenomenon. Women parliamentarians have long been subject to gender-based violence as a means of stifling their political participation, and there is a range of evidence that suggests online violence against women in politics is increasingly escalating into violence offline. IPU estimates that 25% of women have been subject to physical violence during their parliamentary terms, and 22% subject to sexual violence. The risk of such violence impedes women parliamentarians' ability to fulfil their duties freely and securely, and ultimately hinders democracy by deterring women's political participation overall.

ABOUT CPA UK'S WOMEN'S ROADSHOWS

In response to this growing concern, CPA UK hosted three virtual workshops in July 2021, facilitated by Glitch – a UK charity working to end online abuse – and communications consultancy BeSpoke Skills. The three-hour workshops provided parliamentarians with a safe platform to discuss the use of social media as part of their roles and share techniques in building resilience against online abuse.

The successful delivery of these Roadshows shed light on common challenges faced by women parliamentarians, as well as the local and cultural specificity of their experiences of online and offline abuse.

From October to December 2021, CPA UK hosted a second cohort of Roadshows, as part of a project funded by the UK's Foreign, Commonwealth and Development Office (FCDO) to strengthen good governance, parliamentary oversight and accountability across the Commonwealth. Held regionally, parliamentarians from 17 Commonwealth legislatures came together to share their experiences of online and offline spaces as women in politics.

These updated workshops aimed to deliver a programme tailored to each local and cultural context, addressing women parliamentarians' key concerns around online violence and its continuum with violence in the offline space. This included training on digital self-defence, digital citizenship, assertive communication, and safety responses.

ABOUT THIS GUIDE

This handbook follows the August 2021 publication of CPA UK's Guide to Addressing Online Abuse. It serves as an updated practical guide to navigating abuse both online and offline.

From digital self-defence, digital citizenship, to navigating offline threats through assertive communication and safety planning, this handbook paves the way for women MPs to take informed steps to enhance their safety.

While this updated guide cannot reduce the risk to zero, CPA UK hopes it will act as a practical resource for parliamentarians to refer to when developing approaches to managing their online communications and offline safety.

SECTION 1: ADDRESSING ONLINE ABUSE

Digital Self-Defence: Navigating Online Threats

The internet is both a tool that can encourage diverse democratic engagement, and a forum for gendered disinformation, hate speech, abuse, and harassment, targeting politically active women. It is therefore vital that women MPs take steps to enhance their safety and security online. Below are online safety measures designed to reduce risk and vulnerability to all online threats:

1. Secure your devices and accounts

- Set up complex passwords and change them frequently. The National Cyber Security Centre (NCSC) recommend using a sequence of three random words and keeping track of them using a secure password manager.
- Avoid using autofill passwords. Secure password managers have autofill features which are not as easily infiltrated by cyber threats.
- Set up two factor authorisations on Instagram, Twitter and Facebook, as well as your personal and work computers. Two factor authorisations act as a second layer of protection and make it more difficult for attackers to gain access.
- Keep devices up to date. NCSC report that criminals exploit flaws or bugs in software and apps with the aim of getting access to devices or accounts. Using the latest software, apps and operating systems on your devices can fix bugs and immediately improve your security.

2. Keep your location hidden

- Ensure your location settings are turned off and remove social media features that automatically track your live location. Feminist Frequency recommend turning off the camera location on your smartphone, so that your images aren't tagged with your whereabouts.
- You can follow steps to change your apps location settings on Android and Apple.
- Only post on social media revealing details of your location after you have left the venue.
- The National Democratic Institute recommend running weekly check-ups on the privacy settings of your social media apps. You can do this on Instagram, Facebook and WhatsApp.

3. Protect your personal information

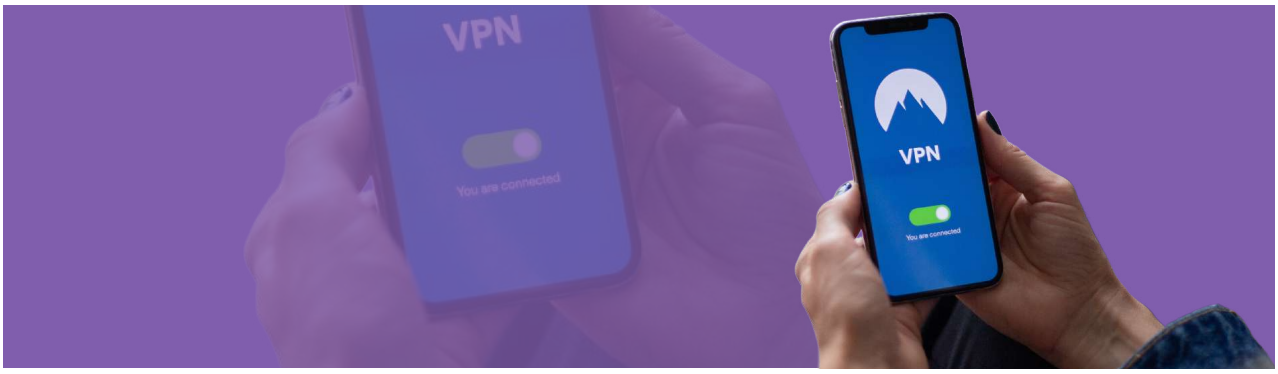
- Ask your family and friends not to share your personal information without your consent. This includes through social media posts, conversations, and/or sharing your exact location. Refer to Pen America's guide on how to talk to your family and friends about online abuse and set boundaries.
- If your home address or personal information is listed publicly, you should take steps to have this taken down.
- The National Democratic Institute (NDI) also recommend using an office address or a rent box at the post office away from your residence, so your home address is not public.
- Do not label any keys with specific identifiers relating to your name or their use.

4. Keep track of your name and information online

- Get one step ahead of potential online abuse and risks to your safety, by immediately identifying any content which is personal and private information and/or likely to provoke online attacks.
- Use Google Alerts to be notified when anything with your name is published online, including any social media handles or alternative names you have used. You can learn how to create an alert here and learn more from Pen America on how to protect yourself from doxing here.
- Glitch recommend using haveibeenpawned.com to see if your email addresses or passwords are compromised online.

5. Audit your social media pages

- Review old posts and clean up your social media pages. This is particularly important if your account has transitioned from a personal account to a political account in the course of your political career. Online trolls frequently target women MPs and sift through their previous posts to expose 'evidence' they are not fit for office. Resurfacing old posts in this manner also exposes women MPs to a further pile on of online abuse.
- Use Facebook's bulk delete tool to make it easier to clean up your posts. In the apps for Android and iOS, tap your avatar (top left), then tap the three dots and choose Activity log. From here pick Manage activity and Your posts to see all your previous posts. Use the tick boxes on the left to select the posts you want to manage.
- Use TweetDelete to bulk delete tweets that are older than one week. You can also remove tweets containing certain words, and have the process run automatically every few days.
- You can read more from Pen America how to audit your social media pages here.



6. Use a VPN

- Use a Virtual Private Network (VPN) to protect your internet connection and privacy online. It allows you to use Wi-Fi hotspots safely by masking your location and encrypts and protects data between your device and the public network. A VPN also limits how governments can track you and reduces the potential of hacking. Glitch recommend using Nord VPN or Express VPN.
- Avoid using public wireless internet connections without a VPN.
- You can read more from Surveillance Self Defence on how to use a VPN here.

7. Encrypt and back up your information

- Store an encrypted backup in a separate and secure place, and let your trusted contacts know where this is. Encryption means converting information or data into a code to prevent unauthorised access. If devices are at risk of confiscation or being searched, encryption is key. Creating a secure backup is also important in case files are corrupted or hacked.
- Use applications such as Sync or pCloud to encrypt and store your information on your behalf.
- In high-risk settings, Glitch recommend using encrypted applications for messages and phone calls, such as Signal.

8. Be alert to gendered disinformation and defamation

- Gendered disinformation and defamation are considered to be an extension of violence against women in politics. To participate in public life, women face the weaponization of information that directly impacts their opportunities for leadership and participation.
- Online gendered disinformation and defamation are generally considered to be hard to deal with under existing laws. However, the majority of countries allow you to bring civil suits under common law around claims of gendered disinformation resulting in defamation. Media Centre have created a resource which provides further information on this.
- If you are a victim of gendered disinformation, document all evidence including screenshots to build a case. Use this form produced by Glitch to support your documentation. This resource provides further information to support you in completing the form.
- NDI have released a guide which addresses gendered disinformation.

9. Create a list of trusted contacts for support

- Identify safe people and places you can go to if you fear for your physical safety. Ensure this is communicated to your trusted contacts and constitutes part of wider personal safety planning relating to online abuse escalating into the offline space (refer to page 15 for further details on this).
- Glitch recommend asking trusted people to report harmful posts and, if they feel comfortable, ask them to respond and/or escalate reports on your behalf.
- NDI also recommend memorising the contact details of your trusted contacts and establishing regular safe and secure check in mechanisms.
- Work to establish a specific point of contact at social media platforms, or a mediatory organisation, with whom you can escalate reports of abusive situations. In non-Western, non-white and non-English speaking contexts, NDI recommend this should be someone with intersectional expertise in both online violence against women in politics and the local context.

10. Document online abuse

- Document all online abuse in order to build a strong evidence base to persuade the police, social media companies and/or governments to take action. It is unfortunate that the onus is on women to document and report online abuse. However, documenting this abuse is important to ascertain when it is necessary to escalate events of abuse to the police.
- NDI recommend using this documentation to identify patterns in who is perpetrating the abuse and what their motivations are.
- Use this form produced by Glitch to effectively document cases of online abuse. This resource provides further information to support you in completing the form.
- Store this form securely and have a backup in place and ensure your trusted contacts are able to access this.
- You can read more from Pen America on documenting online abuse here and assessing the threat level here.

Practicing Self-Care: Managing your Well-Being Online

Social media is a powerful tool for parliamentarians to increase their personal engagement with constituents and to converse directly on the issues most concerning those they represent. This however does not mean that online abuse is a part of the job. Developing and communicating online boundaries is one method that allows women MPs to assert their rights in online spaces, and reclaim social media as a positive and effective tool for digital democracy.

1. Identify and define your boundaries

Identifying and defining your online boundaries involves deciding what online communications you are going to engage in and how you are going to respond to instances of online abuse. Glitch recommend using these online boundaries to inform and develop a page policy for your social media accounts. You can also use these boundaries to inform and develop an internal staff policy for those managing your social media accounts to follow.

2. Form your page policy

Establishing and implementing a page policy for your social media accounts is a key mechanism through which you can reclaim your agency over your digital spaces, by setting clear guidelines on what is and is not acceptable on your page. Key points to consider when forming your page policy include:

- Your page policy should be specific to your social media use and outline the purpose of your social media account, such as to promote local news and events.
- Your policy should clearly communicate what is and isn't acceptable on your account. For example, by including how you will respond to abusive posts or messages.
- Your page policy should outline the consequences of a user violating your page policy, such as the deletion of comments and the user being blocked from your page. Tech Safety recommend having clear and consistent policies around why and how posts or comments are removed, and when an individual will be blocked.
- Glitch recommend creating a 'pinned post' for your page policy at the top of your Facebook page and/or Twitter feed.
- An example of a UK parliamentarians social media page policy can be found here.

3. Implementing your page policy

- If someone violates your page policy, it is important you take action and implement the steps put in place by your page policy. Tech Safety recommend considering informing the person whose post or comments you remove why you did so and remind them of your content guidelines, to demonstrate consistency in your approach.
- If you are unable to block someone for personal or professional reasons, Glitch recommend using Twitter's Advanced filters function which enables you to mute individual accounts. This can also be used to filter specific words or phrases which may frequently be used to abuse you.
- You may choose to respond to the online abuse directly. For some parliamentarians, responding to online abuse might be an important and empowering step in countering online abuse and reclaiming control of online narratives. Alternatively, you may choose to screenshot and share the content without the abuser's username, so as not to incite further abuse while also building awareness.

Pen America's guidelines on safely responding to online abuse:

1. Assess the threat level. Before choosing to confront an online harasser, you should make an honest assessment of the threat level, both in terms of your physical and digital security. Work your way through the questions in the Assessing Online Threats guide and remember: trust your judgment and follow your instincts.
2. Self-evaluate: Am I ready for confrontation? It's not worth confronting an online harasser until you're emotionally prepared to do so. Engaging a harasser when you're highly agitated might escalate the abuse or cause ensuing abuse to have a more harmful impact on your well-being.
3. Decide how and where you want to confront your harasser. Confronting your online harasser does not have to mean sending a direct message or naming the individual abuser. In instances where you're targeted from multiple online accounts, you'll be unable to address specific individuals and will need to confront the abuse more generally.
4. Establish your end goal. Consider what you hope to gain from confronting the abuser. Be prepared that, while you might not change your attacker's mind, you can still set the record straight and become a positive example for others who are being attacked online.
5. Use language and craft messages that are likely to de-escalate the abuse. Condemn the harassment and abuse rather than the harasser; name the consequences and its impact on you; avoid using abusive language; find a way to express your humanness; and show empathy.

For further details on these steps refer to Pen America's guideline here. HeartMob and TrollBusters also offer further advice and support on responding to abuse.

4. Prioritise your self-care and well-being

- It is an unfortunate reality as a woman MP every time you are visible on social media, it is a probable you will be on the receiving end of online abuse in one or more forms. Online abuse is as much of a risk to your wellbeing as offline abuse, and oftentimes poses a real risk of escalating into the offline sphere.
- To pre-empt any emotional toll caused by online abuse, it is important to consider your current state of mind, well-being and physical safety if you were to receive backlash online to a particular post.
- Accordingly, consider delaying posts which may be received as particularly 'controversial' until you feel mentally fit.
- Parliamentarians cannot be expected to be online and accessible at all times. Glitch recommend setting aside time for yourself and your team to sometimes step away from the screen or to pass on social media responsibilities to a colleague if you're handling particularly harmful online abuse.

- Taking care of yourself mentally and physically is critically important for you to continue expressing yourself freely online. Pen America recommends practicing and committing to whatever self-care works for you, such as journaling, mediating, or getting out into nature.
- You can read more from Pen America on self-care in response to online abuse here.

5. Support your team

- Discuss your page policy with your team so they know how to keep you, and themselves, safe online.
- Encourage your team to read this report and follow the safeguarding and safe-care tips.
- Be aware that team members who hold multi-intersecting identities may be impacted disproportionately by online abuse. Glitch recommend encouraging these individuals to pass their responsibilities onto another colleague if the abuse is particularly harmful.
- Create a team social media policy that prioritises staff well-being and allows stepping away from the screen. This could include rotating people on your social media team, having cut off periods by 7pm, or allowing only a certain number of days of social media use.
- Consider what support you can offer your team members if they do face online abuse. Having a list of support services available in your office and/or staff handbook is a useful place to start.
- You can read more from Pen America on how to best protect your team here.

Digital Citizenship: Allyship across the Commonwealth

With growing reports of online harassment across the Commonwealth, it is becoming more crucial that women MPs are equipped with the best methods to support one another. One such way is by becoming an online active bystander and being an uplifting voice to anyone on the receiving end of abuse.

5 ways Glitch recommends you can be an Online Active Bystander:

1. Stop scrolling and be wary and mindful of online abuse when it occurs, rather than immediately scrolling past an abusive post.
2. Support the person experiencing online abuse. Send them a direct message, share your favourite meme or send supportive pictures, and let them know they're not alone.
3. Report the online abuse to the social media company, police or other digital safeguarding or women's organisations that may be able to provide support.
4. Reply to the original post and engage with it as intended. Glitch report this can help to take attention away from the abuse and focus back on what the author originally wanted to discuss.
5. Amplify the voice of the person experiencing the abuse and other marginalised communities, by sharing their post with a supportive message. Glitch state this helps to ensure the voice of the original poster is louder than that of those being abusive and helps to address the silencing effect of online abuse.

For further details on these steps refer to Glitch's guide on being an active bystander here.

Building parliamentary alliances

Supporting other women MPs and demonstrating effective allyship must also extend beyond the online space into parliamentary settings. Building parliamentary alliances is critical to mobilise action around both individual cases of online abuse and broader campaigning on the issue.

Building women's cross-party alliances

Many legislatures across the Commonwealth have networks established for women parliamentarians, such as women's caucuses. Through such groups, members can provide cross-party support on the common challenges they face as women in politics. Beyond enacting gender-sensitive policy, women's parliamentary forums are vital for sharing concerns and creating solutions, particularly in those legislatures where women are a minority.

Building alliances with men

Advocating for the safety of women online is the responsibility of every parliamentarian, and

women parliamentarians cannot advance this agenda alone. This is especially true in contexts where parliaments are dominated by men. For any gender equality agenda to gain ground, it requires their support.

It is therefore vital that women MPs and women's parliamentary groups actively engage with men in raising awareness around their experiences of online violence. Male parliamentarians have a vital role to play in leading by example and demonstrating effective allyship.

Building external alliances

Parliamentarians are in a unique position to engage with a range of actors in the field of online violence. This includes law enforcement, the judiciary, civil society organisations, technology companies, and the media. Building collaborative relationships with actors in each field is key when pursuing action broader legislative reform.

Building alliances in the media, for example, is crucial to ensure the mobilisation of awareness raising efforts, and to ensure messages are communicated beyond the constituency.

SECTION 2: ADDRESSING OFFLINE ABUSE

Reasserting your Rights: BeSpoke Skills on Navigating Offline Threats

Women parliamentarians across the Commonwealth are expected to navigate cultures of aggression and hostility as part and parcel of the job. In the offline world, these cultures are similarly working to discredit and delegitimise their democratic voices. It is therefore vital that women MPs are equipped with the communication skills necessary to reassert their rights.

1. Assertive communication

A key communication skill which enables women MPs to stand up for their rights is that of assertiveness. Applying the principles of assertive communication when navigating offline threats enables you to effectively respond to situations where those rights are being compromised.

Understanding assertiveness

Assertiveness is the ability to convince others of your point of view, to gain acceptance, support, and commitment. Gender biases mean that women are stereotyped as passive and submissive, and men are considered natural leaders – assertive and strong. Women parliamentarians are working against this stereotype everyday simply by existing in politics and advocating for the changes they want to see.

Women MPs' confidence to speak up around issues concerning their personal safety should not be confused with their ability to fulfil their parliamentary duties effectively.

Below are the key tips shared by BeSpoke Skills on using assertive communication to enhance personal security and safety.

Know your rights

One of the first rules of assertiveness is to know what your rights are as an MP. This includes not just your legal rights but also your rights to be heard, to be listened to, to have a different opinion, and ultimately to feel safe. Employers in all workplaces are expected to provide safe working conditions – and parliament is no exception. Knowing what you are trying to convey enables you to be clear in your message and provide others with clarity.

Stand up for your rights

Being assertive means standing up for your own rights in such a way that you do not violate the rights of others - by expressing your needs, wants, opinions, feelings, and beliefs in direct, honest, and appropriate ways. Standing up for your rights means highlighting situations where those rights are being compromised, such as when your prevailing circumstances represent a real risk of danger which you cannot be expected to avert.

Set guidelines

Setting guidelines is essential to assertiveness as they pre-empt any problems or challenges that may arise. They also translate our rights into clear responsibilities and demonstratable behaviours for others. Implementing guidelines can be particularly useful in the context of open discussions around safety and security. Examples of guidelines include:

- Valuing all contributions
- Speaking respectfully in relation to tone and timing
- Challenging appropriately

Set boundaries

You have the right to create your own boundaries. Being passive on this allows others to disregard them. Being passive means failing to stand up for your rights or doing so in such a way that others can disregard them, by expressing your needs, wants, opinions, feelings, and beliefs in apologetic or self-effacing ways. Your safety and security is a non-negotiable boundary which everyone you engage with should respect.

Say no

Knowing your rights is also about understanding that you need to feel mentally fit and resilient to confront a challenging situation and take action. Standing up for this right is also about feeling comfortable saying no - for example, not attending an event because it is not safe. Parliamentarians should not be fearless – this should be balanced against the risks of persevering in the face of threats to your safety and well-being.

2. De-escalation techniques

Assertive communication can be applied not only in delivering your key messages, but also in strategies to de-escalate threatening situations. Awareness of how to respond to immediate threats through de-escalation is key to securing your safety. Below are BeSpoke Skill's key strategies on de-escalation to reduce risk and vulnerability in threatening situations:

Stance: when de-escalating another person, you want to be in a non-threatening, non-challenging and self-protecting position. Ensure you have both feet planted on the ground and appear ready to move quickly by leaning on the front foot. Position yourself at a clear distance, on an angle and off to the side of the other person.

Hand gestures: ensure hand gestures are open and non-threatening and that your hands are always visible. Avoid finger pointing to minimise appearing accusatory or aggressive. Use a self-protective stance by locking your hands in front of you, rather than folding your arms.

Tone: your tone of voice gives subtle but clear ways in which you are telling someone how you expect them to behave. Aggression can escalate aggression, whereas a controlled voice is one of calm and firmness which promotes confidence in both parties. Engaging someone in conversation requires speaking slowly and using a light tone of voice, whereas encouraging someone to step down or move away requires a clear and strong tone of voice to deliver the message.

Questioning: the use of questions is key to encouraging the second party to talk so you have time to process and manage your responses to the situation. If you are seeking to challenge the situation, you can use push back questions such as: Why are you asking? Who is your source?

If you fear for your physical safety, activate your emergency safety plan. Refer to page X for further details on this. It is recommended you call the police or other responsible agency if it is safe to do so.

3. Understanding your mindset and fear

Understanding your mindset and fear is essential to building your judgement and immediate response system when dealing with offline threats. It allows you to ascertain when you are feeling mentally fit and resilient enough to take on a challenging situation, or when you need to divert the situation and take a break. Below are BeSpoke Skills' key tips around understanding your mindset and fear.

Get to know your stress signs

Recognising your individual stress signs is key to predicting when you may reach capacity, particularly as a high level of stress frequently becomes part and parcel of the job as a parliamentarian. Stress signs are also highly personal and may manifest differently in different people. It is important to share these stress signs with your team ahead of any political turbulence.

Balance fear and risk

Oftentimes women parliamentarians overcome fear by focusing solely on driving their mission as an MP. Without reflecting on your mindset, however, this can jeopardise your safety by clouding your judgement and underestimating the risk of threats.

It is therefore important to reflect on your mindset and consider how you are managing fear. Conducting risk assessments (pX) and understanding the danger signs of various scenarios can support you in differentiating between your experience of fear and actual risk.

Protect your team

It is also important to reflect on the mental fitness and resilience of your team. This includes accounting for how members of your team with intersecting identities may experience any political hostility differently and/or disproportionately.

Your team will only be able to support you effectively when they are mentally fit and resilient. Accordingly, it is important to make time to schedule regular check ins and discussions around how you are able to support their needs during any times of political turbulence.

For example, if members of your team experience or witness abuse, take steps to allow them a break to recharge their mental fitness and build resilience.

Build resilience through self-care

Taking regular breaks and prioritising self-care is the key to building and maintaining resilience. Make a commitment to a stress relieving activity and stick to it as much as possible. The more you focus on your well-being, the more capable you will be at successfully fulfilling your duties as a parliamentarian.

Safety Planning: BeSpoke Skills on Emergency Responses

Online violence against women is a continuum of offline violence, and not a separate phenomenon. There is a wide range of evidence that suggests online violence against women in politics is increasingly escalating into violence offline. As a result, it is important women parliamentarians and their staff are prepared in terms of how to respond to a physically threatening situation. One such way is preparing an emergency safety plan.

Although safety plans are highly personal and context specific, basic measures to consider when forming your safety plan include:

- Identify a safe place you can go to in the case of an emergency. Discuss this safety plan with your members of your team, family and/or friends who you have designated as 'safety contacts'.

- Ensure your designated safety contacts are aware of their specific roles in an emergency: this may include taking actions on your behalf, such as childcare or accessing money and essential documents.

- Consider safety measures you can implement within your constituency office and your home which would be useful for an emergency situation. This may include adding additional locks, security cameras and panic buttons.

- Teach and practice a signal for your team to indicate if you or they are in trouble and to activate your emergency plan. Ensure that you change this signal regularly and limit wider knowledge of this signal to a 'need to know' basis.

- Identify a phrase or fact that your designated safety contacts would recognise as proof of life. Limit wider knowledge of this phrase or fact to a 'need to know' basis.

- Review your safety plan weekly and ensure it is up to date with changing circumstances. Ensure any changes to your safety plan are communicated immediately to your designated safety contacts. Where possible, discuss your safety plan and how it will be implemented with your team prior to any high-risk events or journeys. Refer to page X for further details on this.

To develop and establish your own emergency safety plan in full, BeSpoke Skills recommends the OSCAR model to structure conversations with your team:

O – What outcome you want
S – What situations you might be in
C – What choices you have
A – What actions you can take
R - How you might be able to review

Safety Planning for Events: BeSpoke Skills on Preparing for Public Facing Engagements

The IPU reports that 1 in 4 women MPs are subjected to physical violence throughout their parliamentary term. In many cases, this violence takes place when MPs are undertaking vital parts of their jobs, such as holding constituency surgeries and attending political events. It is therefore necessary to take practical precautions to reduce risk and vulnerability in these settings.

Risk Assessments

A risk assessment is a tool through which women parliamentarians can ascertain the level of risk of harm they will be exposed to in their parliamentary roles. It is a systematic examination of evaluation of all aspects of parliamentarians work that considers what/who could cause harm, whether the risks could be eliminated, and if not, what preventative measures should be in place.

The National Democratic Institute have produced the Think10 tool, a questionnaire designed to enable women parliamentarians to conduct a risk assessment and ascertain the level of risk they are exposed to by participating in public life within their jurisdiction. Risks assessments should be regularly conducted to inform and update general safety planning, as well as safety planning in preparation for specific events.

Key questions to consider when conducting a risk assessment in preparation for an event include:

- Who could cause harm: consider who will be attending the event, whether they will be supporters or opponents, and whether the event is open to all members of the public. It is also important to consider the wider political mood and your experiences of constituents and/or members of the public on social media in the weeks leading up to the event.
- Whether the risks could be eliminated: consider the existing safety and security measures available at the event and whether this offers sufficient protection.
- What preventative measures should be in place.

The below tips map out BeSpoke Skill's key recommendations for preventative measures to reduce risk and vulnerability when attending public facing engagements:

Before an event

- Undertake a risk assessment when attending a new venue or new event. Liaise with the venue and/or event organisers to complete this assessment and ensure they are aware of your security needs.
- Get to know the venue layout and discuss with your team how your emergency safety plan would be implemented in this setting.
- Ensure the local police are informed of the dates, times and locations of your surgeries and other events with high levels of public facing engagement.
- Do not provide advanced or detailed information on your wider movements that could enable a person with malicious intent. For example, if you are visiting a range of locations in your constituency, do not provide timings or an ordered list.
- Ensure there is a detailed list of attendees available, by requesting constituents to book appointments or asking members of the public to pre-register for an event. This allows you to verify the identity of constituents and bring any previously problematic individuals to the attention of the team and/or the police. This should include individuals who you have identified as perpetrators of online abuse against you.
- If you will be leaving the venue at night or travelling a long distance, ensure a pre-booked and licensed cab is available.
- Publicise your collective partnership with the venue and police/emergency services, without revealing any exact details of how security measures will be implemented. For example, by stating that security or police may be present without outlining the exact numbers of these personnel.

During an event

- When arriving and departing, remain vigilant and be mindful of the route to and from the venue to a safe place. If you are attending a regular venue, vary the route as much as possible to avoid routines which individuals could identify.
- Where possible, ensure a member of your team is by your side, so that one of you can call for help if necessary. Maintain a line of sight with other colleagues where possible.
- Ensure you have quick access to your mobile phone and emergency numbers are saved.
- Be aware of the nearest exist and position yourself as close to this as possible. Ensure there is always a clear path to this exit.
- Where possible, position a desk or table between yourself and any constituents during public facing events.
- Have a planned exit strategy to use if you feel uncomfortable or threatened. If you fear for your physical safety, activate your emergency safety plan.

After an event

- Following the event, debrief with your team to discuss any concerns or issues arising during the event. Keeping a record of any security issues will allow you to identify patterns and update your emergency safety plan accordingly.
- Consider how the event reflects on the effectiveness of your current pre-event risk assessment and whether this needs to be improved and/or updated.

NEXT STEPS

Through our focus on parliamentary strengthening, CPA UK is committed to empowering women in parliament. During the Roadshow discussions, participants committed to taking action in their legislatures, including sharing the techniques they had learned with colleagues, raising public awareness on the issue of online abuse and establishing a network for women parliamentarians to discuss common challenges.

CPA UK will continue to engage Commonwealth women parliamentarians on the issue of online abuse as well as wider issues specifically impacting women representatives.

ACKNOWLEDGEMENTS

CPA UK would like to thank Glitch and BeSpoke skills for their support in facilitating this round of Roadshows and in the creation of this resource. For more practical tips and resources from Glitch, please read Digital Threats to Democracy or access their website here.

USEFUL RESOURCES

Online Abuse 101 by Women's Media Centre
Addressing Online Misogyny and Gendered Abuse: A How-To Guide by NDI
Think 10 Questionnaire and Guide by NDI
Resources by Glitch
Take Back the Tech
Toxic Twitter by Amnesty International
From impunity to Justice: Domestic legal remedies for cases of technology-related violence against women by Association for Progressive Communications

Africa

Africa Digital Rights Network
Digital Safe tea by Pollicy
ICT Action Network (Kenya)
Maru
Pollicy
Safe Sisters
Alternate Realities, Alternate Internets, African Research for a Feminist Internet by Pollicy
A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda by Pollicy

Asia

Bytes for All (Pakistan)
Bangladesh Women Lawyers Association (Bangladesh)
Centre for Cyber Victim Counselling (India)
Digital Rights Foundation Cyber Helpline (Pakistan)
Gender IT (India)
IT for Change (India)
Troll Patrol in India by Amnesty International
Report on Digital Violence in Pakistan by Digital Rights Foundation
Violence Against Women in Politics, A Study Conducted in India, Nepal and Pakistan by UN Women

Americas

HeartMob
NNEDV Safety Net Project (Canada)
Tech Without Violence (Canada)
Troll Busters
Deplatforming Online Misogyny by Women's Legal and Action Fund
Online Misogyny in Canadian Politics, Project Someone
Trolled on the Campaign Trail: Online Incivility and Abuser in Canadian Politics by University of British Columbia

Caribbean

Life in Leggings
Mapping Gender-Based Political Harassment by ParlAmericas
No! to Online Abuse and Harassment (Barbados)
The Internet Society Barbados Chapter
Violence Against Women and the Use of Information and Communication Technology in Jamacia by Gender IT
Report on Online Harassment and Abuse in Barbados by No! to Online Abuse and Harassment
A Study of Women, Politics, Parliament and Equality in the CARICOM Countries by UNDP

Europe

Glitch
UK Safer Internet Centre
The ripple effect: covid-19 and the epidemic of online abuse by Glitch and EVAW
Unsocial spaces by Refuge
The use of the digital world to perpetrate violence against women and girls by Welsh Women's Aid
Cyber violence against women and girls by European Institute for Gender Equality
Sexism, harassment and violence against women in parliaments in Europe by IPU

Pacific

The Online Hate Prevention Institute (Australia)
eSafety Commissioner (Australia)
NetSafe (New Zealand)
Online Safety Commission (Fiji)
Safer Internet Centre (Fiji)
Technology-facilitated abuse among Aboriginal and Torres Strait Islander women, by eSafety Commissioner Australia
Online hate speech: findings from Australia, New Zealand and Europe, by eSafety Commissioner Australia
Sexism, harassment and violence against women MPs in New Zealand by IPU

CPA UK
Westminster Hall | Houses of Parliament | London | SW1A 0AA
T: +44 (0)207 219 5373
W: www.uk-cpa.org
E: cpauk@parliament.uk