Blocking the Noise

The Political Candidate's Guide to Digital Safety

SOUK
SHOUT OUT UK

Acknowledgements

"What would it mean to your mini-you to be represented?

If you feel it matters, then do something."

This guide was co-designed alongside Wales' diverse communities and political candidates. We have interspersed the text with personal reflections and insights from a range of Welsh voices. We are deeply grateful for the trust they placed in us by sharing their stories, and we hope their insights empower future candidates on their own journeys.

A heartfelt thank you to the organisations that supported the production of this guide: **The Jo Cox Foundation**, **Elect Her**, **Disability Wales**, **Race Equality First**, and to the **Welsh Government** for the funding that made this essential work possible.

Additional Formats of the Guide

Cymraeg

I weld y canllaw yma yn y Gymraeg, **cliciwch yma**.

Easy Read in English

For this guide in Easy Read English, **click here.**

Darllen Hawdd yn y Gymraeg

I weld y canllaw hwn mewn Cymraeg Darllen Hawd,
cliciwch yma

1 Minute Version

On the next page you will find a one minute version of the guide.

1 minute guide

If you only have one minute to look through this guide, here are the five most critical pillars of digital safety and resilience:

1 Separate Your Digital Worlds

Consider establishing a firm boundary between your private life and your public campaign. You can do this by creating dedicated public candidate profiles and setting your existing personal accounts to private. To prevent "digital stalking," do not follow your public profile from your private one; this keeps your family, friends, and past photos hidden from bad actors.

2 Build a Buffer

Protect yourself by staying one step removed from the noise. You can turn off notifications, establish “Digital Sunset” hours, delegate a trusted volunteer, use comment filters or other tools to manage what you see online. You can use platform "panic buttons" like Instagram’s "Limits" or TikTok’s "Filter all comments" to ensure no message goes public without manual approval during a "pile-on."

3 Know the Red Lines for Illegal Activity

Not all online nastiness is a crime, but you must know when it crosses the line. The guide identifies what mis-,dis- and malinformation can look like online, but also where this can veer into specific illegal acts such as intimate image abuse, stalking and harassment and hate crimes.

4 Proactively Verify Your True Voice

With the rise of AI and deepfakes, you can help voters find the real you. Watermark your official videos, list your verified handles on all printed leaflets, and use Multi-Factor Authentication (MFA) on every account. Proactively use social media platforms’ support mechanisms, including reporting tools, to ensure that people can find your true voice online.

5 Stay Resilient

Resilience is a campaign strategy. Constant exposure to online hostility leads to burnout and poor decision-making. Protecting your peace of mind and establishing strategies that work for you are essential to "blocking the noise" and staying resilient throughout the election.

Contents

Acknowledgements 2
Additional Formats of the Guide 3
1 Minute Guide 4

Introduction to Digital Safety

What is this guide for? 6
Why does representation matter in politics? 7
Why is it important to consider how to manage your digital safety? 8
What are some of the basic considerations for digital safety? 9

Online Abuse and Intimidation

How can technology be used to create mis-, dis- and malinformation? 10
What counts as illegal activity online? 11
Online Hate Crimes 12
Illegal AI-generated Content 13
Harassment & Stalking 14
How have others experienced online abuse and intimidation? 15

Managing Online Abuse and Intimidation

How do others manage online abuse and intimidation? 16
How can I manage online trolling, abuse, intimidation and harassment? 17
How can social media platforms support me? 19
What are Operation Ford and Operation Bridger? 21
When should I contact the police? 23
What would be helpful evidence to take to the police? 24
How can the police support me? 24
What support is available for the Senedd 2026 elections? 26
How do others stay resilient? 27

Helpful Links and Community-Specific Resources

Helpful Links and Community-Specific Resources 28
Senedd-Specific Resources 29
Key Organisations 30
Other Useful Links 31
Glossary 32

What is this guide for?

This guide is for candidates and support staff to help **manage online intimidation**, **abuse** and **digital safety**. This guide has been produced by Shout Out UK (SOUK) funded by the Welsh Government's pilot Candidate Diversity Grant, with the support of Elect Her, Disability Wales, Race Equality First and The Jo Cox Foundation and co-designed with diverse communities, prospective candidates, elected officials, support staff and policing teams.

Throughout this guide, you will see direct quotes from those who have experienced online abuse and intimidation so you can hear first-hand from their experiences and how they blocked the noise.

"When people see that they can be represented in politics, they are so much more likely to be able to think that they can do it themselves."

Why does representation matter in politics?

"A girl stopped and she said, 'Oh my god, you look like me.' ... that to me was everything."

"One in five people in Wales are disabled. And how can you know people are making decisions on behalf of us who may not actually have a clue about what it's like to be disabled? "

"People deserve a diversity of options and choices for who they want to serve them. This also matches the diversity and representation in our society now."

"I've got a younger sister and I don't want her to think that she couldn't do it if she wanted to"

"Representation leads to better laws and better protections for the people who need it."

"Representation is a self-fulfilling cycle... people are disaffected with politics... because they don't see themselves represented."

"Candidate diversity is absolutely a necessity for a functioning democracy."

"Representation links to trust — if people don't feel represented by their politicians they are less likely to trust them and the system as a whole"

"If people feel represented, politics means something to them. It makes politics more personal. However, diversity shouldn't trump candidate appropriateness, depends on the person."

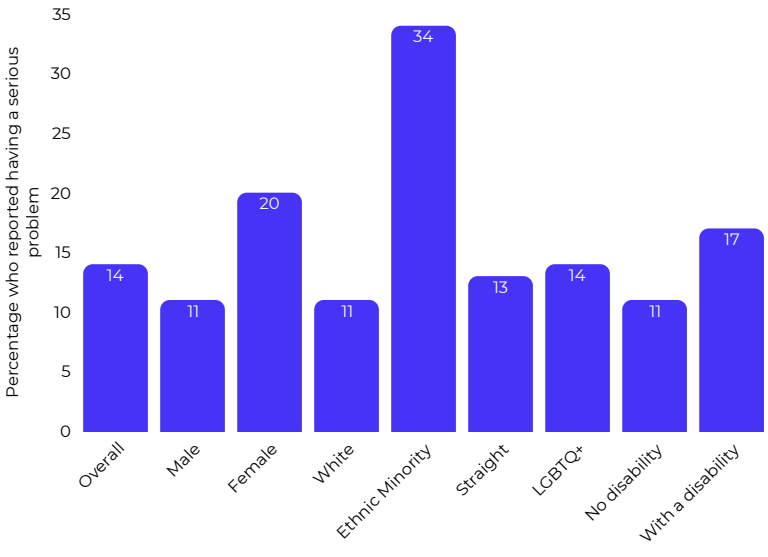
Why is it important to consider how to manage your digital safety?

The Speaker's Conference on the security of MPs, candidates and elections found that:

- **96% of current MPs** have personally experienced **one or more incidents of threatening behaviour** or communication since they began working as an MP.
- When MPs were asked, "**what makes you feel most at risk?**" The most common answer was "**online abuse**".

The Electoral Commission also produced a **Report on the 2024 UK Parliamentary general election and the May 2024 elections**, and found that the online space was more often than not where candidates experience harassment, intimidation and threats.

It is important to note that threats of harm are more common among Black, Asian or minority ethnic MPs and disabled MPs and threats of sexual violence disproportionately affect women and disabled MPs.



Digital Safety

The practice of securing your personal data and digital footprint to prevent physical and privacy risks, while actively managing your online environment to protect your well-being during the campaign.

Online abuse

Targeted digital communication, such as harassment, hate speech, or disinformation, intended to cause emotional distress or damage a candidate's reputation.

Online intimidation

The use of digital platforms to threaten or coerce a candidate, creating a credible fear for their physical safety or the safety of their family and staff.

What are some of the basic considerations for digital safety?

Before launching your campaign, establish a firm digital foundation. The **National Cyber Security Centre** offers guidance to stay secure online. Familiarising yourself with the technology you will be using, and considering a digital plan early prevents personal data leaks and manages your exposure to online noise.

- **Separate Your Digital Worlds:** Set up a new, specific “public” profile for your candidacy. Keep your personal accounts private so your historical data (like tagged photos) isn't accessible to the public.
- **Avoid Account Linking:** Do not follow your "public" profile from your "private" one. This prevents bad actors from finding your private account through your "Followers" list.
- **Define Team Roles: If you have support, clearly allocate responsibilities for who will:**
  - Pre-approve and post content.
  - Monitor and respond to comments.
  - Decide when to report content to platforms or the police.
- **Establish a Verification Strategy:**
  - **Official Channels:** Clearly list your official website and social media handles on all printed campaign literature so voters can distinguish your voice from imposters.
  - **Watermarking:** Use a consistent logo or watermark on official videos and images to make them harder to misappropriate or edit.
- **Secure Your Access:** Use a password manager and enable 2-step verification (Multi-Factor Authentication) on every account to prevent hacking. For guidance on how to do this, head **here**.

“My advice will always be if you’ve got someone managing your online accounts it should be done by one person so you’ve got a consistency of understanding.”

How can technology be used to create mis-, dis- and malinformation?

With recent technological advances, it's easier than ever to create legitimate-seeming disinformation. Some of the ways that mis- and disinformation can be created are:

- **Deepfake video:** An AI-generated video that convincingly replaces a person's likeness or actions with another's to show them doing or saying things that never actually happened.
- **Deepfake audio:** Synthetically generated speech that perfectly mimics a specific person's voice.
- **AI-generated video/images:** Visual media created from scratch by artificial intelligence based on text prompts, often used to create realistic but entirely fictional scenes or videos.
- **AI chatbots:** Computer programs like ChatGPT or Gemini, but also less established chatbots, that use artificial intelligence to simulate human-like conversation and respond to complex questions in real-time. These can sometimes amplify misinformation.
- **Bot accounts:** Automated social media profiles controlled by software rather than humans, often used in election interference to rapidly spread misinformation or artificially inflate certain political narratives.
- **Doxing:** *(also spelt 'doxxing')* The malicious act of gathering and publicly releasing a person's private information, such as their home address or phone number, to encourage harassment or physical threats.
- **Trolling:** The act of posting deliberately inflammatory, offensive, or off-topic messages online to provoke an emotional reaction or disrupt productive political discussion.

Misinformation

False information that may be shared by mistake or misunderstanding, without any intention to deceive. e.g. someone sharing a post about a politician, not knowing the information is false.

Disinformation

False or misleading information that is intentionally created and spread with the purpose of deceiving, manipulating, or misleading others. e.g. somebody creating false information about a politician.

Malinformation

Information that is based on reality, used to inflict harm on a person, social group, organisation or country. e.g. somebody leaking personal information about a politician.

What counts as illegal activity online?

"The vast majority of these people would never say these comments in the street... but they think because they're sitting behind a keyboard, they can just put what they want."

It is perfectly legal to express opinions, disagree, and debate online. Some individuals will take disagreement further into online harm. Although some of this online harm is legal, it is important to understand when opinions and actions online can veer into illegal and criminal action.

Examples of **legal activity** can include:

- Online posts/comments disagreeing with you, your party's policy etc. including consistent messages such as trolling
- Rude and/or insulting posts and comments about you personally, and/or your family or friends
- The creation of AI-generated images that show mis- and/or disinformation
- The use of bot accounts to promote political messages, spread disinformation, and other legal activities online

Examples of **illegal activity** can include:

- Intimate image abuse, including the creation of sexual deepfake images
- Threats to your safety and/or your family and friends
- Stalking and harassment, both online and in-person
- Blackmail, extortion and sextortion

In the next section, we will now go into specific forms of illegal activity online in more detail.

Online Hate Crimes

A hate crime is defined as 'Any criminal offence which is perceived by the victim or any other person, to be motivated by hostility or prejudice based on a person's **race** or perceived race; **religion** or perceived religion; **sexual orientation** or perceived sexual orientation; **disability** or perceived disability and any crime motivated by hostility or prejudice against a person who is **transgender** or perceived to be transgender.'

Evidence of the hate element is not a requirement. You do not need to personally perceive the incident to be hate related. It would be enough if another person, a witness or even a police officer thought that the incident was hate related.

Incitement to hatred
The offence of incitement to hatred occurs when someone acts in a way that is threatening and intended to stir up hatred. That could be in words, pictures, videos, music, and includes information posted on websites.

Hate content may include:

- messages calling for violence against a specific person or group
- web pages that show pictures, videos or descriptions of violence against anyone due to their perceived differences
- chat forums where people ask other people to commit hate crimes against a specific person or group

"As a racialised person, you get it on a different level... someone said they were going to pull my skirt up and rape me. I've reported things about hate crime in the past and I know how to report it. It takes bravery to even report it and follow through to be fair because it's like PTSD when you do it again and you explain to another person. But what I've developed over the years now is a really strong support network."

Illegal AI-generated Content

Intimate image abuse or “revenge porn”

- It is illegal to create, share, or threaten to share intimate photos or deepfakes without permission. This includes asking others to create fake intimate content of another person.

Hate crime

- It is illegal to use AI-generated content or deepfakes to stir up hatred or call for violence against specific groups or individuals. This includes any media designed to be threatening or to promote physical harm.

Fraud

- This involves using AI or deepfakes to deceive you for personal gain. Examples include tricking you into giving up money or revealing private, sensitive information.

Disinformation

- Creating false AI content to cause serious emotional or physical harm or community unrest can be a criminal offence. These cases are often more complex to prosecute than other forms of digital abuse.

Terrorist activity

- Any deepfake or AI content that promotes, glorifies, or assists in carrying out acts of terrorism must be reported to the police. This includes material supporting violent extremism.

Stalking and harassment

- Using AI-generated content to repeatedly alarm, distress, or threaten someone is a reportable offence. It applies whenever such actions make a person feel unsafe.

Blackmail

- Using deepfakes to demand money or forced actions is a crime, often referred to as "sextortion" when it involves sexual imagery. This includes threatening to release fake compromising media unless demands are met.

Harassment & Stalking

Stalking and harassment is when someone repeatedly behaves in a way that makes you feel scared, distressed or threatened. If this unwanted behaviour happens two times or more, it may be a crime and you can report it to the police.

If someone has behaved towards you in a way that's made you feel scared, distressed or threatened and it's happened once it could be antisocial behaviour, hate crime or another offence.

"Most online abuse comes in the form of harassment; persistent and repetitive comments from people who disagree with the party."

Harrassment

Harassment may include:

- sending abusive text messages or images
- posting abusive messages on social media
- making unwanted or offensive phone calls

It's harassment if the unwanted behaviour has happened two times or more and made you feel distressed or threatened.

Stalking

Stalking is a form of harassment, but the stalker will have an obsession with the person they're targeting and their repeated, unwanted behaviour can make the victim feel distressed or scared.

Stalking may include:

- following someone
- going uninvited to their home
- hanging around somewhere they know the person often visits
- watching or spying on someone
- identity theft (signing-up to services, buying things in someone's name)
- writing or posting online about someone if it's unwanted or the person doesn't know

It's stalking if the unwanted behaviour has happened two times or more and made you feel scared, distressed or threatened.

How have others experienced online abuse and intimidation?

Report it

If you've been a victim of any of these crimes, it is understandable that you could be feeling alarmed, distressed or embarrassed.

If you think you are, or may have been, a victim of a crime, there are things you can expect from the police and ways to access support. We understand it takes courage, but reporting to the police is the first step. For more guidance on reporting, head to the reporting section of this guide.

"The vast majority of these people would never say these comments up in the street... but they think because they're sitting behind a keyboard, they can just put what they want."

"Online abuse does not respect normal working hours, and the need to check social media whilst at home, means it affects the well-being of the entire household."

"When you are that candidate and reading online, you think, the immediacy of abuse or harassment is someone around the corner, but the reality might look something a little bit different"

"It gets quite exhausting because there's a lot of trolling"

"Talking about specific issues sees a huge increase in engagement from bots and a spike in hateful comments"

"Political illiteracy transfers over to misguided criticism. When people are not really necessarily sure of who's responsible for what, they will vent out to whoever is publicly available."

"If I say I'm not worried about people putting up photos, videos and comments online, I'd be lying because I am."

How do others manage online abuse and intimidation?

"Replying to a negative comment is not going to help, the other person will only come off feeling either more angry or vindicated."

"Working with people and a party that share my values mean that I'm secure in what I'm doing being the right thing and that makes coping much easier."

"The problem with actively monitoring and seeking abuse is you could just spend your time forever paranoid looking for things. I think nobody's got time for that at all."

"Try to be your own person, don't be afraid to get things wrong. Most important - start small, focused, don't try solve everything on day one."

"Some of my party peers will attack somebody back, but I don't because I'm not online to have a fight with somebody. I don't think it works because I think that the algorithm picks it up and spreads it further."

"Hateful comments are a reflection of those who leave them, not those that receive them."

"Having separate political accounts is so important... you need a differentiation between them."

"Understand how the platform works, understand what the reporting mechanisms are. Be aware how to contact those platforms in advance."

How can I manage online trolling, abuse, intimidation and harassment?

Managing Your Online Presence

While online abuse is a likely challenge for candidates, most incidents involve repetitive harassment or AI-generated vitriol rather than physical threats. Developing a clear management strategy allows you to maintain a professional digital presence without constant exposure to harm.

Establish a First Line of Defence: You can delegate social media monitoring to a trusted volunteer or staff member to filter out abuse. Use platform tools like comment filters to block specific words and provide an automatic barrier. In the next section you will see how to do this across platforms.

Use AI for Safe Summaries: Instead of reading through individual comments and insults, you can use AI assistants to summarise constituent feedback. This keeps you informed about public concerns while avoiding the direct impact of "digital noise."

Set Clear Rules of Engagement: Define what content will be removed and when users will be blocked. Focus your energy on genuine conversations rather than engaging with trolls. Some candidates choose to keep these rules internal while others share these on their social media pages.

Anticipate the News Cycle: Expect surges in bot activity or hateful comments during polarised news events. Prepare for these spikes by tightening filters or stepping back from social media in advance.

"Think of people who are being hateful as victims of misinformation ... it's a way of thinking about it that is less threatening to you."

On the next page you will find further strategies related to your well-being and safety.

How can I manage online trolling, abuse, intimidation and harassment?

“have boundaries and coping mechanisms for hate, but accept there will be some hate that comes with the role given the context we're in right now”

Managing Your Well-being and Safety

Resilience is a campaign strategy; protecting your mental health is essential to preventing burnout during intense periods.

Consider a "Digital Sunset": Set specific hours or days to disconnect entirely from notifications. Turning off "pings" prevents the overwhelming feeling of constant incoming negativity.

Posting Safely: To ensure physical safety, avoid "live-posting" your exact location. Share photos and updates only after you have left a venue.

Protect Your Inner Circle: Be cautious about featuring family, friends or children in campaign materials, as they may become secondary targets for online abuse.

Attend Safety Briefings: As a candidate you can attend safety briefings hosted by local police and your Returning Officer. Establishing this contact early ensures you have a direct line of support if incidents escalate.

How can social media platforms support me?

This section is designed to help a candidate familiarise themselves with the safety features of each platform and take control of their digital environment.

Different platforms have varied features available. It's helpful to consider which tools will be useful in setting up your account (**proactive features**) to mitigate the risk of abuse online and other tools (**reactive features**) that allow you to respond if/when abuse occurs.

Proactive features include **comment filters** which allow you to automatically block abusive comments or comments that include specific words. Some candidates do not moderate comment sections, others choose to set up comment filters and others choose to disable comments entirely. In terms of reactive features, all platforms allow you to **block** and **report** content and accounts. Some platforms, such as Facebook and Instagram, also allow you to respond to crisis situations by temporarily locking your account in case of a virtual mob, known as dog-piling.

"Understand how the platform works, understand what the reporting mechanisms are. Be aware how to contact those platforms in advance."

How can social media platforms support me?

Platform	Proactive Features	Reactive Features
Facebook	• Specific guidance for candidates • Verify your account • Comment Filter	• Report content • Block an account • Manage comments • Lock your profile
Instagram	• Verify your account • Comment Filter	• Report content • Block an account • Manage comments • Lock your profile
X (Twitter)	• Verify your account • Mute accounts or words	• Report content • Block an account • Manage replies and tagging
TikTok	• Register as a candidate and get verified • Comment Filter	• Report content • Block an account • Manage comments
LinkedIn	• Verify your account	• Report content • Block an account
YouTube	• Verify your account • Comment settings	• Report content • Block an account
Bluesky	• Verify your account	• Report content • Block an account

This platform-specific guidance is correct as of March 2026.

What are Operation Ford and Operation Bridger?

Operation Ford

Operation Ford is part of the Defending Democracy Policing Protocol, which commits the UK Government to funding a dedicated named police contact for raising concerns and liaising on security. This operation was initially set up for councillors and other locally elected members, and as of March 2026, has been expanded to protect a broad range of democratic representatives and candidates across the UK.

Operation Ford covers:

- **Candidates** standing for local and devolved elections (this includes Senedd Elections, Local Government Elections, Scottish Parliamentary elections)
- **Devolved Elected Representatives:** Members of the Senedd (MSs) and Members of the Scottish Parliament (MSPs)
- **Elected Local Councillors** (County, City, and Borough level)
- Directly **Elected Mayors** (including Metro Mayors)
- **Police and Crime Commissioners**
- **Staff and Families:** The protection extends to incidents where staff, volunteers, or family members are targeted as a way to intimidate or harass the candidate because of their political role

Under Operation Ford, you are protected through:

- A **Force Elected Official Adviser (FEOA)**: A named police contact in your local force who provides security briefings and safety advice.
- A **National Intelligence Unit:** A specialised team that monitors reports to identify and monitor individuals who target politicians across different areas.
- **Priority reporting:** By quoting "Operation Ford" when you call 101 or 999, your case is automatically flagged for specialists rather than being treated as a standard call.

Does it feel like the situation could get **heated** or **violent** very soon? Is someone in **immediate danger**? Do you need **support right away**?
If so, please call **999** now.

Quote "**Operation Ford/Bridger**" if this is in relation to your political role.

What are Operation Ford and Operation Bridger?

Operation Bridger
Similar to Operation Ford, this is a security protocol, but it is reserved for parliamentary candidates and elected MPs. Instead of a Force Elected Official Adviser, they will have a Dedicated Superintendent who acts as a Single Point of Contact.

Operation Bridger covers:

- **Members of Parliament (MPs)**
- **Candidates** who are running for Member of Parliament
- **Staff and Families:** The protection extends to incidents where staff, volunteers, or family members are targeted as a way to intimidate or harass the candidate because of their political role

Under Operation Bridger, you are protected through:

- **Dedicated Superintendent:** Every police force in the UK has a dedicated Superintendent who acts as the "Bridger SPoC" (Single Point of Contact).
- **Physical Security Funding:** It provides access to funding for standardised security measures at MPs' homes and constituency offices (like CCTV, reinforced doors, or alarm systems).
- **SOS Fobs:** High-risk individuals are sometimes issued GPS-enabled "SOS fobs" that provide a direct, silent link to police dispatch.
- **A National Intelligence Unit:** A specialised team that monitors reports to identify and monitor individuals who target politicians across different areas.

	Operation Ford	Operation Bridger
Elected Representatives	Senedd (MSs), MSPs, Councillors, Mayors, PCCs.	MPs (Members of Parliament)
Candidates	Those standing for Senedd, Scottish Parliament, or Local Councils	Those standing for UK General Elections.
Police Contact	Force Elected Official Adviser (FEOA).	Dedicated Superintendent Single Point of Contact.

When should I contact the police?

Official Guidance from the Electoral Commission:

The actions and behaviours listed below may constitute a criminal offence and should be brought to the attention of your local police. **CPS guidance on responding to intimidating behaviour in elections and public office** provides more detail and information on types of criminal offences, for example:

- Communications, on or offline, which contain abusive or threatening language.
- Repeated unwanted contact may constitute harassment or stalking.
- Racial, homophobic or other discriminatory abuse or threats.
- Fixation on you or an issue associated with your campaign.

The following indicators ('red flags') may signal an escalation and should be brought to the immediate attention of your local police (dial 999):

- Threat of imminent violence.
- Fixated ideas – if someone seems set on a certain course of action or is making a very specific type of threat or reference to a plan.
- If you become aware that the individual has access to weapons or has weapon skills.
- If the person releases personal information about you not already in the public domain.

To read the Electoral Commission's full guidance about harassment and intimidation, **click here**.

In case of an **emergency:**

- call 999

Quote **"Operation Ford/Bridger"** if this is in relation to your political role.

In case of a **non-emergency:**

- call 101 or report online

Quote **"Operation Ford/Bridger"** if this is in relation to your political role.

Still not sure about when to report online content to the police?
https://reportharmfulcontent.com/when-should-you-go-to-the-police/

What would be helpful evidence to take to the police?

For all crimes, having as much evidence as possible is helpful for the police to conduct an investigation and advise you better. You might consider doing some of the following:

- Creating a folder to document evidence
- Taking screenshots or screen-recordings of profiles, posts, comments, videos, etc,
- Documenting dates and times of contact
- Providing as much context as you can around any specific incidents

Remember, links might be helpful, but these can be taken down. Consider screenshotting/screenrecording posts or comments that you wish to show the police.

"Is it hurtful words or is it criminal? A lot of the stuff will be hurtful."

How can the police support me?

As all other individuals in Wales, you have access to your local police services. As a candidate, you have added the support of being covered by Operation Bridger and Operation Ford. As an elected official, you will have additional access to other support mechanisms, such as Senedd security, security services in Westminster or local authority security teams.

Safety briefings - Your local police task force will be holding safety briefings that you will be invited to through your local Returning Officer. These can help you gain a better understanding of local support, threats and issues that will support you to campaign safely online and offline. They can also be a helpful way to understand who your point of contact is.

Sharing information - Online abuse can feel extremely targeted, personal and potentially make you fearful of escalation. Reporting it could potentially offer you further context. Some online trolls are already known to the police and target many candidates and representatives continuously. These individuals might not be from your local area, or even the UK at all.

“I think having a buddy almost, maybe someone who isn't running but someone who you can kind of offload to. I think making sure that you have good people around you is really important.”

Talking with offenders - When you report a crime, the police will discuss each individual case with you and what some options might be. In some cases, speaking with the individual who has perpetrated the online crime might be the best approach.

Prosecuting online crimes - Prosecuting criminal activity online can sometimes lead to a case being passed onto the justice system. Although prosecuting online activity is notoriously challenging, you never know how your particular case fits into other cases or wider policing activity. Reporting illegal online activity, even if it doesn’t lead to prosecution, can strengthen policing in this area.

Please note that during the dissolution of parliament, the Senedd security team will not be available for support. If you need support from the Police, you should ring 999/101 as appropriate.

What support is available to you for the Senedd 2026 elections?

- **Guidelines for Candidates and their Agents** - This includes a Candidate guide overview, but also specific guidance on whether you can stand for election, imprints, spending and donations and others: https://www.electoralcommission.org.uk/guidance-candidates-and-agents-senedd-elections
- **Becoming a Member of the Senedd** - This page provides candidates for election to the Senedd with background information on standing for election, and outlines of the support and guidance that will be available to them if elected. https://senedd.wales/work-opportunities/becoming-a-member-of-the-senedd/#:~:text=Commission%20staff%20provide%20various%20types,for%20constituency/regional%20office%20costs.
- **Diversity and Inclusion Guidance for Registered Political Parties** - This is voluntary guidance for registered political parties: https://www.gov.wales/diversity-and-inclusion-guidance-registered-political-parties-html
- **Access to Elected Office Fund Wales** - The Access to Elected Office Fund Wales, delivered by Disability Wales and funded by the Welsh Government, supports disabled candidates in local and Senedd elections by covering disability-related, non-campaign costs. It funds reasonable adjustments like personal assistants, BSL interpreters, and assistive technology to remove barriers to participation: https://www.disabilitywales.org/projects/access-to-elected-office-fund-wales/

"I'll go in anyone's house and have a cup of tea with them and I just thought I want to put other people first."

How do others stay resilient?

"I want the person down the street from me to know that they have someone to contact if they can't get something in place so that they can get home from the hospital."

"I don't want big press or my name in lights. I want my community to be able to function."

"What would it mean to your mini-you to be represented?

If you feel it matters, then do something."

"Nobody goes into politics because they love politics. They go into politics because they want to make a difference for humans."

"Understand that lot of criticism and hate towards you is because people are upset about their own situations.

"Well-behaved women rarely make history. I need to keep reminding myself of it because that gives a bit of confidence."

"People say they go into politics for glamour but I go into it to sort the bins out"

"It is a lot easier than people make it look genuinely because when I was contemplating it, I was like, 'Oh my gosh, these people are so experienced. It must be so hard.' And it is hard in areas, but genuinely is not half as hard as it looks."

"Just making sure that you're nourishing your body... taking a break... doing self-care... not pushing myself to the ends of the earth."

Helpful Links and Community-Specific Resources

This Candidate Resilience Guide aims to support individuals to be resilient online, through practical guidance based on the lived experiences of those who have stood as candidates, supported others to do so, and have become elected officials. Below, you will find resources and guidance from government bodies that go into further detail, provide training opportunities and will allow you to stay up-to-date with the latest guidance.

UK Government Candidate Security Guidance - This collection of guidance on the government website provides an overview of what candidates and political staff need to know, as well as signposting to more detailed guidance https://www.gov.uk/government/collections/candidate-security-guidance-collection#i-am-a-candidate-how-can-i-improve-my-security

Electoral Commission guidance - The National Police Chiefs Council, working with the Crown Prosecution Service and the Electoral Commission, have produced guidance for candidates and campaigners, to help you understand when behaviour goes beyond political debate and may be unlawful. https://www.electoralcommission.org.uk/our-guidance/candidate-or-agent/guidance-about-harassment-and-intimidation

Senedd-Specific Resources

- **Guidelines for Candidates and their Agents** - This includes a candidate guide overview, but also specific guidance on whether you can stand for election, imprints, spending and donations and others: https://www.electoralcommission.org.uk/our-guidance/candidate-or-agent/senedd-elections-use-elections-taking-place-or-6-may-2026

- **Becoming a Member of the Senedd** - This page provides candidates for election to the Senedd with background information on standing for election, and outlines of the support and guidance that will be available to them if elected. https://senedd.wales/work-opportunities/becoming-a-member-of-the-senedd/#:~:text=Commission%20staff%20provide%20various%20types,for%20constituency/regional%20office%20costs

- **Diversity and Inclusion Guidance for Registered Political Parties** - This is voluntary guidance for registered political parties: https://www.gov.wales/diversity-and-inclusion-guidance-registered-political-parties-html

- **Access to Elected Office Fund Wales** - The Access to Elected Office Fund Wales, delivered by Disability Wales and funded by the Welsh Government, supports disabled candidates in local and Senedd elections by covering disability-related, non-campaign costs. It funds reasonable adjustments like personal assistants, BSL interpreters, and assistive technology to remove barriers to participation: https://www.disabilitywales.org/projects/access-to-elected-office-fund-wales/

- **Dignity and Respect Guidance** - Including how to make a formal complaint about a Member of the Senedd, relating to dignity and respect: https://senedd.wales/help/complaints/dignity-and-respect-guidance/

Key Organisations

Jo Cox Foundation:

- **Resources to address abuse in politics -** https://www.jocoxfoundation.org/our-work/respectful-politics/resources-to-address-abuse-in-politics/

- **Joint Civility Pledge with Compassion in Politics –** https://www.jocoxfoundation.org/our-work/respectful-politics/civility-pledge/

- **Jo Cox Civility Commission Report and Recommendations –** https://www.jocoxfoundation.org/our-work/respectful-politics/commission/

Elect Her:

- **Digital Self Defence, in partnership with Glitch -** a self-guided course to support all women with the tools and knowledge to feel confident using their voice both online and offline https://www.elect-her.org.uk/resource-hub/content/digital-self-defense

Race Equality First:

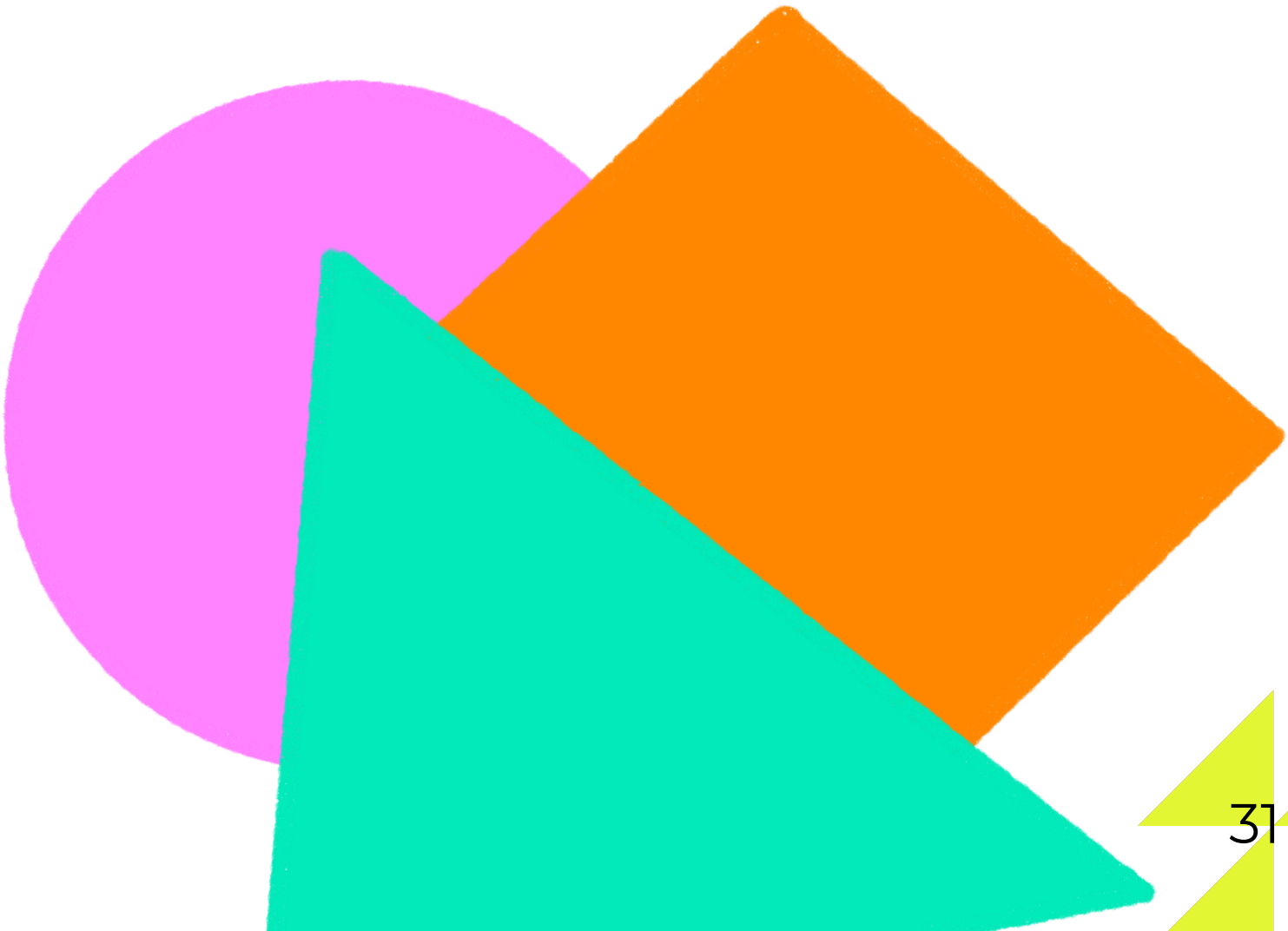
- **Representing Wales: Empowering Community Leaders -** To learn more about this programme to increase the representation of Black, Asian, Minority Ethnic and Refugee individuals in Welsh political and civic life https://raceequalityfirst.org/projects/representing-wales-empowering-community-leaders

Are you struggling to cope? Do you need urgent support?

- **NHS 111 Wales** (Option 2): For immediate, 24/7 mental health support, you can call 111 and select option 2. This connects you with a mental health worker in your area.
- **C.A.L.L. Mental Health Helpline**: A dedicated Welsh helpline providing confidential emotional support, available 24/7. Call 0800 132 737, text "help" to 81066, or visit callhelpline.org.uk.
- **Samaritans Cymru:** Available 24/7 for anyone needing someone to talk to. Call 116 123 for free.

Other useful links:

- **One Voice Wales:**
  - https://www.onevoicewales.wales/training/
- **Safer Politics Toolkits:**
  - https://saferpolitics.org/
- **National Cyber Security Centre:**
  - **Staying Secure Online Guidance:** https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online
  - **Defending Democracy Guidance:** https://www.ncsc.gov.uk/collection/defending-democracy
- **Local Government Association:**
  - **Digital citizenship: support and resources for councillors:** https://www.local.gov.uk/our-support/guidance-and-resources/civility-public-life-resources-councillors/handling-abuse-and-0
- **Mental health resources:**
  - **Mindfulness courses and support**: https://valleyssteps.org/
  - **Mental health helpline for Wales:** https://callhelpline.org.uk/
  - **NHS 111**: https://111.wales.nhs.uk/?locale=en&term=A
  - **Samaritans Cymru:** https://www.samaritans.org/samaritans-cymru/



Glossary

- **AI Chatbots:** Computer programs that simulate human-like conversation and can sometimes inadvertently amplify misinformation.
- **Bot Accounts:** Automated social media profiles controlled by software, often used to spread misinformation or create a manufactured appearance of support or hatred.
- **Deepfake:** AI-generated video or audio that convincingly mimics a person's likeness or voice to show them doing or saying things that never occurred.
- **Digital Safety:** The practice of securing personal data and digital footprints to prevent privacy risks while actively managing your online environment for wellbeing.
- **Digital Sunset:** A strategy for maintaining resilience by setting specific times or days to stop checking notifications and disconnect from online noise.
- **Disinformation:** False or misleading information that is intentionally created and spread with the specific purpose of deceiving or manipulating others.
- **Dog-piling:** A situation where a "virtual mob" or a large number of users coordinate to flood an account with abuse, often triggered by a viral post.
- **Doxing/doxxing:** The malicious act of gathering and publicly releasing a person's private information, such as a home address, to encourage harassment.
- **Harassment:** Unwanted behaviour, such as sending abusive messages, that happens two or more times and makes a person feel distressed or threatened.
- **Malinformation:** Information that is based on reality but is leaked or used specifically to inflict harm on a person, group, or organisation.
- **Misinformation:** False information that may be shared by mistake or misunderstanding without any underlying intention to deceive.
- **Multi-Factor Authentication** (MFA), also known as **2-step verification**: A security process requiring both a password and a secondary code (sent to a phone or email) to confirm your identity during login.
- **Online Abuse:** Targeted digital communication, including hate speech or harassment, intended to cause emotional distress or damage a reputation.
- **Online Hate Crime:** A criminal offence perceived to be motivated by hostility or prejudice based on race, religion, sexual orientation, disability, or transgender identity.

Glossary

- **Online Intimidation:** The use of digital platforms to threaten or coerce a candidate, creating credible fear for their physical safety or that of their family.
- **Operation Bridger:** A national security protocol providing protection and a dedicated Superintendent point of contact specifically for MPs and UK Parliamentary candidates.
- **Operation Ford:** A policing protocol that provides a named Force Elected Official Adviser (FEOA) to support the security of local and devolved candidates and representatives.
- **Stalking:** A form of harassment driven by an obsession, involving repeated, unwanted behaviour that makes a victim feel scared or threatened.
- **Trolling:** The act of posting deliberately inflammatory or offensive messages online to provoke emotional reactions or disrupt productive discussion.

Bibliography

Crown Prosecution Service. (2024). Responding to intimidating behaviour in elections and public office: A CPS guide. https://www.cps.gov.uk/publication/responding-intimidating-behaviour-elections-and-public-office-cps-guide
Electoral Commission. (2024). Report on the 2024 UK parliamentary general election and May 2024 elections. https://www.electoralcommission.org.uk/research-reports-and-data/our-reports-and-data-past-elections-and-referendums/report-2024-uk-parliamentary-general-election-and-may-2024-elections#abuse-intimidation
Electoral Commission. Guidance about harassment and intimidation. https://www.electoralcommission.org.uk/our-guidance/candidate-or-agent/guidance-about-harassment-and-intimidation
Electoral Commission. Guidelines for candidates and their agents — Senedd elections. https://www.electoralcommission.org.uk/our-guidance/candidate-or-agent/senedd-elections-use-elections-taking-place-or-6-may-2026
Home Office. (2024). Defending democracy policing protocol. https://www.gov.uk/government/publications/defending-democracy-policing-protocol/defending-democracy-policing-protocol
National Cyber Security Centre. Top tips for staying secure online. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online
National Cyber Security Centre. Defending democracy guidance. https://www.ncsc.gov.uk/collection/defending-democracy
Welsh Government. Diversity and inclusion guidance for registered political parties. https://www.gov.wales/diversity-and-inclusion-guidance-registered-political-parties-html
Senedd Cymru. Becoming a Member of the Senedd. https://senedd.wales/work-opportunities/becoming-a-member-of-the-senedd/
Senedd Cymru. Dignity and respect guidance. https://senedd.wales/help/complaints/dignity-and-respect-guidance/
Disability Wales. Access to Elected Office Fund Wales. https://www.disabilitywales.org/projects/access-to-elected-office-fund-wales/
Report Harmful Content. When should you go to the police? https://reportharmfulcontent.com/when-should-you-go-to-the-police/
Local Government Association. Digital citizenship: support and resources for councillors. https://www.local.gov.uk/our-support/guidance-and-resources/civility-public-life-resources-councillors/handling-abuse-and-0
Jo Cox Foundation. Resources to address abuse in politics. https://www.jocoxfoundation.org/our-work/respectful-politics/resources-to-address-abuse-in-politics/
Jo Cox Foundation. Joint civility pledge with Compassion in Politics. https://www.jocoxfoundation.org/our-work/respectful-politics/civility-pledge/
Jo Cox Foundation. Jo Cox Civility Commission report and recommendations. https://www.jocoxfoundation.org/our-work/respectful-politics/commission/
Elect Her / Glitch. Digital Self Defence: a self-guided course for women. https://www.elect-her.org.uk/resource-hub/content/digital-self-defense
Race Equality First. Representing Wales: Empowering Community Leaders. https://raceequalityfirst.org/projects/representing-wales-empowering-community-leaders
One Voice Wales. Training. https://www.onevoicewales.wales/training/
Safer Politics. Safer Politics Toolkits. https://saferpolitics.org/

Interviews
Anonymous interviewees. Interviews conducted by Shout Out UK. Wales, 2026. Testimonies drawn from diverse Welsh communities, prospective candidates, elected officials, support staff, and policing teams. All participants anonymised.

SOUK

SHOUT OUT UK