Dealing with digital threats to democracy: A toolkit to help women in public life be safer online
Introduction

At Glitch, we want women to feel safe to use their voices online as well as offline at all stages of their political career, whether a student activist, a campaigner, an elected official or someone seeking to stand.

We’ve created this toolkit to help you look after yourself online and to support those around you. It offers our top tips on staying safe from online abuse – an umbrella term for various tactics and malicious behaviours experienced in digital spaces.

Why is this needed?

We hear worrying stories of online abuse being directed at women in public life. Amnesty International’s Troll Patrol project found Members of Parliament (MPs) have experienced many forms of online abuse. Women are 27 times more likely to be targeted, a figure that increases for those with marginalised intersecting identities who are faced with abuse based on, for example, disability, gender, race, religion and sexual orientation. Specifically, Black women are 84% more likely to receive abusive tweets than white women.

Online abuse has a real impact in offline spaces. Research has revealed that online abuse is one reason many women MPs choose not to run for re-election. This is a threat to our democracy. By using and sharing this resource you’re helping to make online spaces safer for all.

1. Amnesty International UK (2018), Troll Patrol
4. Amnesty International UK (2018), Troll Patrol
5. Collingnon and Rüdig (2020), Harassment and Intimidation of Parliamentary Candidates in the United Kingdom
How to get started

Use this toolkit as an audit or checklist, and schedule time to return to it regularly, perhaps with your friends or colleagues. It will help you and your team to:

Practise digital self-defence and self-care

Become an online active bystander to support those experiencing online abuse

Keep your supporters safe online
Glitch @GlitchUK_ • 13:08
I will help fix the glitch to end online abuse #FixtheGlitch #DigitalCitizen
Enable two-factor authentication in settings for your work and personal email accounts. Each time you log in, you’ll need a code (sent to you as a text/phone call or via an app), making the log-in process doubly secure.

Have separate work and personal phones if you can. Avoid dual-sim phones – they seem convenient, but you might make the mistake of using a personal sim card for work messages or posts.

Install anti-virus software and firewalls to defend your data from malicious activity.

Use a screen lock on all devices but avoid ‘pattern unlock’ methods which are easy for strangers to copy when you’re out and about, such as working from a café or checking your phone on the train. Don’t use birthdays or anniversaries as passcodes – they are not secure, especially if the details are already online such as in your bio or photos of a celebration.

Get set up securely

**Turn on two-factor authentication?**
- [ ] Text message: use your phone to receive a text message
- [ ] Authentication App: use an authentication app to get a verification code

Working in the public eye means sharing your political views with a wide audience. People will connect with you, retweet you, comment with their support. But others will try to use online platforms to challenge your campaign in an unacceptable way. Taking these simple steps to stay safe online will help you feel confident to use your voice in every situation.
DIGITAL SELF-DEFENCE

How to use digital tools during your political career

Only use public Wi-Fi through a VPN (virtual private network), downloadable from providers such as ExpressVPN or NordVPN. Data between your device and the public network will then be encrypted and protected.

Use security settings like the Find My app and Android Device Manager. If your device goes missing, you’ll be able to track its location and disconnect it from your accounts.

Support your team to take the steps above and to:

- avoid auto-login options when managing multiple accounts, e.g. an MP’s email account plus a staff one.
- create unique, secure passwords for each account – password manager software will autogenerate these and store them securely.

Watch out for scams and emails sent from identical fake accounts. Use a simple three-step check:

1. Be wary of emails from anyone you don’t know, emails with lots of obvious grammatical errors or anything that doesn’t look right.
2. Hover your cursor over links and email addresses to make sure they are genuine.
3. Ask a colleague or friend for their view.
I will help fix the glitch to end online abuse #FixtheGlitch #DigitalCitizen
DIGITAL SELF-DEFENCE

How to use digital tools during your political career

Stay safe on social media

- Create a second social media account for your public role and use a nickname or alias for your personal accounts.

- Stay secure by switching on auto-updates (or set a reminder to install security updates every few weeks).

- Keep your privacy settings updated so only people you know can see your personal accounts. Remove anyone you are no longer in touch with.

- Hide your location by not using features such as Facebook check-in, Snapchat geofilters or Instagram location tags/stickers; wait until you have left the area. If you use these features, strangers can track your live location – that may not be safe for you, your team, or your supporters.

Remain vigilant

- If you see news about a data breach for a company you have an account with, update your account details and passwords. Check haveibeenpwned.com regularly to see whether your information has been compromised.

- Follow developments in technology and related government legislation, for example, support the Online Harms Bill and follow Glitch on social media.
DIGITAL SELF-CARE

How to look after yourself and your team online

Taking care of yourself is not a luxury; it is a necessity. How much better do you feel if you’ve had a good night’s sleep, got some fresh air or had a chat with a friend? It’s the same online – we all need to protect our mental health and well-being by taking simple actions that make a positive difference to how we feel.

Create online boundaries

Use a page policy or pinned tweet explaining what you will/won’t engage with online. Create this with your team so you’re all aware of these boundaries

Get comfortable using the block and report functions on apps like Facebook and Instagram, plus the mute and filter options on Twitter. Establish a policy on how and when to do this – train your team so they feel confident about what to do

Spend some time offline

Take breaks from social media or ask someone in your team to take over if they can, especially at very stressful moments. Delete the app off your phone (you can reinstall it when you’re ready to go back) and do something you enjoy, e.g. get outside, arts and crafts to keep your hands busy, read a book or call a friend

Create a simple policy that lets team members know it’s okay to step away for a time or to pass the social media account they’re managing to a colleague if online abuse is particularly triggering or harmful. This is especially important if people in your team hold multi-intersecting identities as they may already be impacted disproportionately by online abuse outside of work
When you see someone being harassed at work, on the street, on a train, what do you do? Show kindness to the person being targeted. It’s no different online.

You can show support by sending an encouraging message and reporting the abuse. We know it seems easier to call out the abuser. To try to make them apologise. But any negative language just perpetuates the cycle.

Put your energy into becoming an online active bystander – making the victim feel seen and heard. We can all play our part in creating safer online spaces.

**To become an online active bystander:**

1. Help people report abusive posts or comments to the relevant social media companies
2. If you know someone is being unfairly targeted, be their ally by replying to them and engaging with their post in a positive way
3. Send an encouraging message, image, video or GIF
4. Encourage people to document the abuse and help report it to their line manager, supervisor or another responsible person with a duty of care
5. Create healthy allyship by sharing resources you find helpful on your professional and personal accounts
Fill in the blank

1. _____ is to experience online abuse in the UK.
2. Globally, men are _____ times more likely to experience harassment online than women.
3. Black women are _____% more likely to be monitored in problematic and abusive contexts.
4. _____% of girls admitted to censoring themselves online because of fear of abuse.
Tips to share with supporters

Help your supporters champion good digital citizenship and create a safer internet for all. Run through these tips at your next meeting or share this whole resource.

Keep safe online

- Be wary of quick sign-ups when setting up social media. A longer process with some basic ID verification like a mobile phone number means safer interactions and fewer fake accounts.

- Avoid lots of personal details on your social media and dating profiles. The less information you share about yourself and where you are, the more secure you’ll be.

- Never share financial information or transfer money via a social media or dating app.

- Report online community groups that don’t comply with social norms.

- Become an active online bystander: report posts and links on social media that have harmful content or misinformation.

- Share these tips with others to create safer online spaces for all.
Tips to share with your supporters

Look after yourself

If you experience online abuse, talk to someone you trust, such as a friend or family member, about what’s happening and how it makes you feel. Ask them to listen and support you, not escalate the abuse or disclose more of your private information.

Ask friends and family to help you document the abuse (take screenshots or use our form on fixtheglitch.org), ask them to report it for you or with you (including to the police if necessary by calling 101).

Take time for yourself each day. Balance the challenges of being online by doing something you enjoy.

Write a page policy, pinned tweet or short post that lists what you expect from others online. It’s a great way to protect your well-being by making people aware of your boundaries. It could include how you’ll respond to abusive messages and how you’ll engage with anonymous accounts, trolls and topics that aren’t up for debate.

You can also create your own privacy checklist to call to mind when you’re next posting. Ask yourself questions like: does this post contain private or personal information I don’t want to expose? Am I comfortable sharing this with all my followers?
Fix the Glitch Toolkit Training

Fixtheglitch.org

@GlitchUK  @Glitchuk  @UKGlitch

GLITCH
7 Steps to a Positive Public Campaign

1. **CREATE COLLECTIVE ACCOUNTABILITY**
   and safe spaces online and offline by outlining collective principles for your campaign that you will hold yourself and others accountable to.

2. **STAY ON TOPIC**
   and engage the public by discussing issues and policies, not people or personalities. Focus on solutions and frame things positively.

3. **LEAD BY EXAMPLE**
   by using respectful language when addressing abuse, especially when it comes from your own supporters.
7 Steps to a Positive Public Campaign

4. Design safety into your strategy to proactively mediate discussions prompted by your campaigning.

5. Use digital self-care tools to help you deal with abuse and stay in control: you can mute, block and filter content. Remember to take a break whenever you need to.
SET & COMMUNICATE PERSONAL BOUNDARIES

that enable you to give your best to the campaign while protecting your home life, and the privacy of you and your loved ones. Boundaries could include agreeing: times of day you’re uncontactable; what you will engage with online; only to discuss your campaign through official channels such as email or your public social media accounts.

BUILD A COMMUNITY

of trusted allies you can lean on and celebrate with. Think about how to create a collective where you all support and uplift each other.
Thank you for joining our community of digital citizens making online spaces safer.

Please share this toolkit with your networks. And let us know how you get on with putting these tips into practice – how have they made a difference? What have you found challenging? Is there anything else that could help?

Ask us about our bespoke workshops for political parties, marginalised communities and women and campaigners in public life. We will support you and your team to develop your own tailored plan and gain the skills and confidence to use your voices online.

Email info@glitchcharity.co.uk – we’d love to hear from you.
Dealing with digital threats to democracy has been created by the Glitch team – Seyi Akiwowo, Gwen Taylor, Hayle Chalke-Davies, and Kiran Chalke co-developed the content with support from Layla Austin.

We would also like to thank:

Luminate, who empower people to work together to build fairer societies, for the pivotal funding for the toolkit and Schillings, experts in protecting people’s reputations and privacy, who supported and advised on its development.

The Gender Institute at Royal Holloway, University of London, especially Dr Sofia Collignon for sharing her research and helping develop the toolkit, and Professor Sarah Childs for her support and advice.

Simran Nanuwa (@merakiscreenprints on Instagram), for the design, and Hazel McCoubrey (@hazelmccoubreyillustration), for the wonderful illustrations.

Pip Rowson for additional copywriting, editing and proofreading.
About Glitch

We’re a UK charity committed to ending the abuse of women and marginalised people online. Through workshops, training, reports and programmes, we equip our intersectional community to become the digital citizens we need in the world today. From grassroots to systemic change, we advocate for online spaces that are safe for all.

An important note on using this toolkit

Although Glitch is a charity, we’ve made this toolkit freely available so we can reach and support as many people as possible. In return, we ask that you adhere to our Creative Commons license – you must not edit or alter this resource, nor use it for commercial gain. If you’d like permission to translate the toolkit, get in touch.

Follow us online

@GlitchUK_  glitchcharity.co.uk
@GlitchUK_  info@glitchcharity.co.uk

Dealing with digital threats to democracy by Glitch is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Glitch is a registered charity in England and Wales 1187714