SAFER.POLITICS

Online safety for political communication staff

Introduction

With social media being a crucial part of your role as a politician, the toolkit and accompanying training module are designed to help keep you safe online. Whether you have just been elected or have been a councillor for a number of years, there should be something here for all when it comes to using social media as part of your role.

The toolkit is designed to support all levels of experience, from those who have never used social media before to those who are confident and long-term users.

While there are numerous benefits to using social media, there are potential pitfalls to be aware of, including online abuse which some politicians have faced. Representatives across the political spectrum have experienced homophobic, racist, gender-based or ableist abuse, which can lead people to leave politics or deter them from entering politics in the first place. The potential chilling effect that such behaviour can have on democracy has prompted researchers at the University of Liverpool to conduct a range of studies into this issue which has informed the production of this resource.

Things to consider before you start

It is important to note that if you are experiencing online abuse then you should alert colleagues and, where appropriate, police. You should also alert the social media platform in question.

Social media is an important tool for you as a member of staff involved in communication activities for an MP / prospective parliamentary candidate, enabling you to communicate and engage with constituents and key stakeholders.

This online safety toolkit aims to support you in using it as safely as possible and in knowing what to do and where to go if you or your colleagues experience any online abuse.

It has the benefit of enabling you to share key messages and updates on your MP or prospective parliamentary candidate's work without the need to go through a gatekeeper such as a journalist. It also enables you to respond directly to any questions which constituents may have.

Equally, there are a number of potential pitfalls and risks when it comes to using social media. An important thing to bear in mind here is that social media can be overwhelming, with messages and comments flying around at all times of the day and night.

As such, it is crucial to set boundaries to help protect yourself and to ensure your colleagues support each other in making best use of social media as part of your campaigning and work.

Agree on the times when you or your colleagues will be checking in on your account/s. It is a good idea to include this in your MP / PPC's bio. Any users should then be aware when they might reasonably expect a response from your accounts.

Vigilance against cyber attacks

As someone who is part of a team supporting a politician or PPC in a high profile role and privy to sensitive information, you are at greater risk of cyber attacks.

Among the potential means of cyber attack is something known as spear-phishing. This is when a communication is sent to a particular person and is designed to look like it has come from a known or trusted contact.

These can be sent to personal email addresses as well as business email addresses. Malicious links can be included in such emails through a URL or can be embedded into a document on something like Google Drive.

The victim can then be directed to a fake sign in page for what appears to be a legitimate service. Their details will then be used to sign into their own account and to forward any future correspondence to the cyber attacker.

If in doubt about whether an email is genuine then check via a different means. Also do a regular check to ensure there is no mail forwarding active on your account.

Be very careful about what, if any, personal information you and your colleagues share via social media. It could be used as part of a spear-phishing attack. Cyber attackers will often gather and use such information to devise persuasive and convincing emails.

Likewise, be cautious about connecting with people on social media, even when they appear to have mutual contacts. They could be fake accounts, set up to impersonate others.

You should use a professional social media management service, which will enable colleagues to create posts without the need for password sharing.

Using a social media management tool enables an audit trail to be kept in terms of who has posted content. If using a social media management tool, ensure that account access logging is switched on, if it is available.

You should also implement a content approval process, setting out how any draft social media content will be checked and signed off to guard against any problematic content.

Only authorised staff should have access to your MP / PPC's social media accounts and social media management tools. Ensure that such access is removed before any staff members leave their role and change any passwords which they had access to.

You should also ensure you have an emergency recovery plan in place. This should set up what to do, for example, if a colleague or anyone with access to your MP / PPC's accounts has posted damaging content.

You need to know who to contact in advance of any such situations arising.

Ensure devices are locked when not in use.

The National Cyber Security Centre advises the use of three different words combined to make a stronger password. This renders it more difficult to hack and easier for you to remember.

Tips on making the most of social media

Set boundaries

Ensure you set clear boundaries as to when social media followers and users can expect a response from you. You may want to put this in your bio.

Take breaks

You cannot and should not monitor social media for extended periods of time or outside of your specified social media monitoring hours, unless, of course, an emergency arises. Ensure that you take regular breaks and if you have experienced online abuse then you are entitled to come away from your social media accounts for the sake of your own health.

Be cautious when it comes to revealing your location

Think about whether you need to post your location. However tempting it may be to post photos of you and your team out and about canvassing, in some situations, it is best to do so after the event. Be aware that, for example,Don't posting a picture of where you will be canvassing saying, e.g. "we'll be out until 3 in THIS AREA" can. This has been known to attract threats and even in-person incidents, so think carefully before you publicise your location. This can also be done for other events you might be speaking at.

Posting in this way has the twin-advantage of avoiding issues of seeming like you haven't been active, which can draw criticism and abuse, but keeping you and everyone in your group safe.

Know how and when to report to each platform and police

Familiarise yourself with what kinds of abuse you can report and the reporting features of each platform. Be mindful that most platforms have no function to link multiple replies into one report. They often only let you add posts on the user's feed - not replies to you. So if there are repeated responses from one account there may need to be separate reports which can be upsetting. If this happens, it can be helpful to get assistance from a trusted friend or colleague to gather the relevant material for reporting.

If you think it may become a police matter then screenshots are always best as deletions / bans are common. You should also screenshot the user's bio to get proof of settings, ie that what they posted is or was in the public domain. If you suspect someone has set up new accounts after a ban then do your best to document e.g. similar language / emoji use.

As before, you should enlist help with documenting, if need be, so as to protect yourself from the messages.

Proof read before pressing publish

Always ensure you proofread - or ask a colleague to cast their eyes over what you have written - before publishing. This should help avoid errors such as the unfortunate hashtag used to launch singer Susan Boyle's new album - #susanalbumparty - intended to be read as Susan Album Party.

Vigilance against cyber attacks

As someone in a high profile role and privy to sensitive information, your MP is at greater risk of cyber attacks.

Among the potential means of cyber attack is something known as spear-phishing. This is when a communication is sent to a particular person and is designed to look like it has come from a known or trusted contact.

These can be sent to personal email addresses as well as business email addresses. Malicious links can be included in such emails through a URL or can be embedded into a document on something like Google Drive.

The victim can then be directed to a fake sign in page for what appears to be a legitimate service. Their details will then be used to sign into their own account and to forward any future correspondence to the cyber attacker.

If in doubt about whether an email is genuine then check via a different means. Also do a regular check to ensure there is no mail forwarding active on your MP's account

Be very careful about what, if any, personal information your MP shares via social media. It could be used as part of a spear-phishing attack. Cyber attackers will often gather and use such information to devise persuasive and convincing emails.

Likewise, caution your MP to be careful about connecting with people on social media, even when they appear to have mutual contacts. They could be fake accounts, set up to impersonate others.

Consider using a professional social media management service, which will enable you and your colleagues to create posts without the need for your MP to share their passwords.

Using a social media management tool enables an audit trail to be kept in terms of who has posted content. If using a social media management tool, ensure that account access logging is switched on, if it is available.

You should ensure a content approval process is in place, setting out how any draft social media content will be checked and signed off to guard against any problematic content.

Only authorised staff should have access to your MP's social media accounts and social media management tools. Ensure that such access is removed before any staff members leave their role and change any passwords which they

had access to.

You should also ensure that an emergency recovery plan is in place. This should set up what to do, for example, if an employee or anyone with access to your MP's accounts has posted damaging content.

You need to know who to contact in advance of any such situations arising.

Ensure that you and your colleagues and your MP lock any devices when not using them.

The National Cyber Security Centre advises the use of three different words combined to make a stronger password. This renders it more difficult to hack and easier for you to remember.

https://www.security.gov.uk/guidance/social-media-guidance/

https://www.security.gov.uk/guidance/social-media-guidance/using-social-media-securely

https://www.security.gov.uk/guidance/social-media-guidance/perform-social-media-security-assessment

Guidance on recovering a hacked account:

The National Cyber Security Centre

https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

For more information on protecting what you post on social media, visit:

https://www.ncsc.gov.uk/guidance/social-media-protect-what-you-publish

Reporting a cyber attack

You can report any cyber attack incident via the link below:

https://report.ncsc.gov.uk/

Setting up a social media use and harassment protocol with your MP/party

It is important to agree a social media and harassment protocol so that your MP and colleagues are aware of what to do in the event of any online abuse and how to help safeguard the team from any such abuse.

The agreed boundaries in terms of social media and online content can then be shared with social media users to make clear what is acceptable behaviour and what will not be tolerated.

Two examples of such protocols, taken from the websites of Labour MP Jo Stevens and Conservative MP Stuart Anderson can be seen below.

Labour MP for Cardiff East Jo Stevens's website and social media policy

"This website and associated social media channels – **Instagram**, **Facebook**, **X (formerly Twitter)**, **LinkedIn** and **TikTok** – are managed by members of Jo Stevens MP's team. They are designed to share news, photos, and resources about Cardiff East, including what your MP is doing in the constituency and Parliament – and how you can get involved.

"We want these online spaces to be a safe places for people – particularly constituents of Cardiff East – to share their comments and thoughts on the issues covered here. To make sure our online community is a safe and enjoyable environment for people to comment, question and engage in debate, we ask everyone to follow these community guidelines:

1. We encourage respectful discussion between people. You don't have to agree with what other people say or share, but please treat everybody with dignity, courtesy and respect.
2. Comments expressing any of the following will be removed and reported by our moderators:
   a. Discrimination based on race, ethnicity, national origin, religion, sexuality, sex, gender, age or disability
   b. Advertising or promotion of any services or pages
   c. Unintelligible spam or comments that are not relevant to the topics raised on the page, or the same comment(s) on multiple posts
   d. Violence or harm towards MPs, our moderators, or anyone else on our page
   e. Misinformation and conspiracy theories
   f. Comments from fake accounts or bots that seek to hijack the comments
3. Our moderators will decide which comments break these guidelines, and will hide and delete any comments that do, as well as block any users who do not follow the guidelines.
4. To keep comment moderation manageable for our moderators, we will limit the public reply and comment functions on some posts.
5. We may also report harassment and malicious communication to the police if needed.

"As always, if you live in Cardiff East and have an issue you would like to raise directly with your MP, please email: **jo.stevens.mp@parliament.uk**, ensuring you include your full name and address as Parliamentary rules mean that this office is only able to represent constituents of Cardiff East. Thank you."

South Shropshire Conservative MP Stuart Anderson's social media protocol

"I am proud to have been elected as the Member of Parliament for South Shropshire. I am keen to hear from and engage with as many residents as possible, and have already engaged with many through surveys online, by email, out campaigning, attending local events and hosting my own 'Meet the Candidate' events.

"I use social media to promote my activities and priorities as I campaign, raising local issues as well as national Conservative policies. I know that I hold political views not everyone will agree with. I also know that others will have their own views and opinions that I may not agree with. I respect this. Even if I don't agree with someone's views, it is still their right to hold them.

"That said, it is incumbent upon all of us to discuss political issues with respect and moderation. No one should feel intimidated or threatened, online or offline. There are a number of ground rules that I have set for my social media channels. These have been designed to ensure that all interactions uphold the principles of mutual respect and common courtesy. Sadly, there are some who wish to abuse my social media for their own purposes. I do not believe that this is right. I do not do this to others with different viewpoints. I have a right to protect myself from any threats of harassment and abuse.

"My social media channels are my own platform, owned and curated by myself and/or select people who help manage my social media. While I will occasionally respond to comments, these platforms are not an appropriate place to raise matters that need an in-depth response. Comments are not a substitute for emails, and I won't be able to respond in the same way. It is best to send your enquiry as an email to **stuart.anderson.mp@parliament.uk**.

"The ground rules that I have set for my social media channels are as follows:

1. As I have mentioned above, the primary purpose of my social media accounts is to champion local issues and promote my work in Parliament on behalf of my constituents. If you are identified as not living or working in the constituency, you may have your comments ignored, hidden, or removed.
2. Abuse and threats of any kind will not be tolerated – even if you think that the words you used were mild or posted with tongue in cheek. Any comments that are felt not to be polite or respectful may be hidden or deleted without prior notice. The account that is posting them may also be blocked and reported to the social media companies and to the Police accordingly. I have a zero-tolerance policy, which means all threats and abuse will be reported straightaway to appropriate authorities.
3. Whilst I welcome feedback, the comments sections of my social media channels are not to be used by opposition activists or organisations to post their own political views. As long as they follow the rules set by the social media company, they should be able to create their own page or account.
4. Likewise, comments that are intended to deflect or divert attention from the content of the main post may be removed without prior notice.
5. Spamming is not tolerated. This includes persistent posting of comments across multiple posts or platforms that say the same thing or an unrelated comment to the original post. These comments will be deleted and the account that is posting them may be blocked without any prior notice.

6. Advertising of any kind is not permitted and any genuine recommendations of products or services that people make in the comments are the responsibility of the person making the recommendation.
7. No issues should be raised on my social media that accuse or insinuate an individual or organisation of wrong doing or of a confidential nature. These should either be raised directly with the police or emailed to myself at **stuart.anderson.mp@parliament.uk**"

What to do when you witness harassment/experience it by proxy

If you or your colleagues witness harassment or experience it by proxy, then you need to take the following steps depending on the situation.

If you or your colleagues feel threatened by online abuse then you should notify police. You should also notify colleagues and the relevant social media platform.

It is crucial that you take steps to protect yourself by calling on colleagues, for example, to help with any of these steps. In terms of ensuring you have sufficient evidence of any online abuse, you will need to take steps such as screenshotting the posts or direct messages in question.

You should also take screenshots of the home page of that particular account to prove, for example, that it was publicly accessible at the time any abusive material was posted. This is a necessary precaution in case the account is locked down or even deactivated or deleted at a later date.

It is important to add here that if you believe that you - or someone you know - is in immediate danger then you should contact police on 999.

Non-emergency situations, which do not require an immediate police response, should be reported by dialling 101.

Further guidance on when you should contact police is included here: https://reportharmfulcontent.com/when-should-you-go-to-the-police/.

For more information on stalking and harassment, visit **https://www.police.uk/advice/advice-and-information/sh/stalking-harassment/what-is-stalking-harassment/.**

Impact on mental health

If online abuse if impacting your mental health then it is crucial that you take a break. You also have the option of deleting a social media account.

Some social media platforms allow you to temporarily deactivate accounts.

For more information on online harm and how to report it visit **https://reportharmfulcontent.com/.**

We would advise doing an online check by putting your MP / PPC's name into a search engine and seeing what comes up.

You can check if an email has been involved in a data breach by visiting **https://haveibeenpwned.com/.**

Phishing emails

Beware of phishing emails which can appear, at first glance, to be from official organisations. Alternatively, you may get emails which appear to be from a constituent, with an urgent sounding request to open malicious links. Phishing emails are designed to enable the sender to install malware, which is malicious software used to steal personal data or money.

The check a website service can be used to check if a website is genuine. It has been set up by the government-supported Get Safe Online site in partnership with the Cifas fraud prevention service.

https://www.getsafeonline.org/checkawebsite/

Ensure that apps are regularly updated to ensure they have the latest fixes and security updates.

Useful links for further information

Setting up two-step verification

https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv

Documenting online abuse

https://www.onlinesos.org/

Meta - Facebook / Instagram / WhatsApp / Threads

Meta safety center

https://about.meta.com/actions/safety

Crisis support resources (you need to select UK in drop-down menu)

https://about.meta.com/actions/safety/crisis-support-resources

Online safety for women in government

https://www.facebook.com/government-nonprofits/blog/online-safety-for-women-in-government

Meta's guidance on what happens when AI or digital methods are used in political or social issue ads

https://www.facebook.com/government-nonprofits/blog/political-ads-ai-disclosure-policy

Guidance for prospective politicians

https://www.facebook.com/government-nonprofits/best-practices/candidate

Tips to protect your MP's Facebook and Instagram accounts

https://www.facebook.com/government-nonprofits/blog/tips-to-protect-your-facebook-account

LinkedIn

https://www.linkedin.com/help/linkedin/answer/a1337839/?lang=en

TikTok

https://newsroom.tiktok.com/en-us/protecting-election-integrity-in-2024

https://www.tiktok.com/safety/en/safety-privacy-controls/

TikTok's community guidelines

https://www.tiktok.com/community-guidelines/en/

WhatsApp

Staying safe on WhatsApp

https://faq.whatsapp.com/1313491802751163

X (formerly Twitter)

https://help.twitter.com/en/safety-and-security

YouTube

https://support.google.com/youtube/topic/2803240?hl=en&ref_topic=6151248

Force elected-official advisors

Every police force has a force elected-official advisor (FEOA) to support MPs, councillors and candidates in terms of their personal safety while campaigning for office.

They can also offer support for police and crime commissioners and metropolitan mayors during any elections.

FEOAs can provide briefings on personal safety while candidates are campaigning and the Electoral Commission has advised that candidates should maintain contact with them throughout the election process.

The government has advised that any candidates experiencing harassment or intimidation and believing there to be an immediate threat to their safety should call 999.

In the case of what the government describes as a less immediate threat, candidates are advised to call 101 or visit police.uk.

In a press release issued by the government on 25 April 2025, National Police Chiefs' Council lead for Policing Elections Deputy Commissioner Nik Adams said: "As with every election, the police's role is to prevent and detect crime, and enable the democratic process to take place.

"We take that role very seriously because intimidation of candidates and their supporters has serious implications for individuals and wider democracy.

"We want every candidate, and everyone involved in securing the democratic process, to know that we are here to help them and keep them safe.

"All candidates will receive security advice and guidance from their local force. We would encourage candidates to read this guidance and attend security briefings.

"They should also take the time to introduce themselves to their local force, and ensure they know who their point of contact is. It is also important to take practical steps when campaigning to ensure safety.

"There have also been briefings from partners in related fields, such as around personal security, risks that come from social media, and general cyber safety advice.

"We would encourage candidates to be as proactive when engaging with our partners as much as they would be with the police."

Online Safety Act 2023

The Online Safety Act 2023 protects children and adults online. It passed into law on 26 October 2023.

Ofcom is leading on implementing the Act's provisions.

A number of new criminal offences were introduced by the Act and came into effect on 31 January 2024. The government has stated that these cover:

- encouraging or assisting serious self-harm

- cyberflashing
- sending false information intended to cause non-trivial harm
- threatening communications
- intimate image abuse
- epilepsy trolling

These offences apply directly to the individuals sending them, with convictions already made under the cyberflashing and threatening communications offences, the government has said.

More information about the Online Safety Act 2023 can be found at **https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer**.

Further reading

National Cyber Security Centre's guidance for high-risk individuals on protecting your accounts and devices

https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals

https://www.ncsc.gov.uk/guidance/guidance-for-individuals-in-politics

https://www.nwci.ie/images/uploads/NWC_Toolkit_SocialMediaAbuse_2022FINAL.pdf

A handy glossary explaining some of the key social media terms is available via the Get Safe Online site

Glossary - Get Safe Online

The Glitch charity

https://glitchcharity.co.uk/wp-content/uploads/2022/09/Dealing-with-digital-threats-to-democracy-PDF-FINAL-1-1.pdf-1.pdf

The Jo Cox Foundation

https://www.jocoxfoundation.org/our-work/respectful-politics/commission/recommendations/

Social media civility and respect guide produced by Breakthrough Communications on behalf of the Civility and Respect Project

https://docs.google.com/document/d/1iftaoflxjGqrMj4kSiua_G3Ih-E_wfR6onmemLR9rL0/edit#heading=h.xubrbixchv8m

The Safer Politics website has been produced by the University of Liverpool's Centre for Digital Politics, Media and Democracy in co-operation with the Local Government Association.