SAFER.POLITICS

Online safety for local political candidates and representatives

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 consider alerting the social media platform in question.*

Social media are important tools for you as a local councillor / prospective local councillor, enabling you to communicate and engage with your 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 experience any online abuse.

Social media enable you to share key messages and updates on your work without the need to go through a gatekeeper such as a journalist. They also enable you to respond directly to any questions your constituents may have, if you choose to use them this way.

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.

It can be helpful to establish rules about when you will be checking in on your account/s, and what kinds of messages will receive a reply. It is a good idea to include this in your bio. Any users should then be aware if and when you might reasonably be expected to respond.

Some councillors make it clear in their bio that any requests for support need to be made via email rather than social media.

The Local Government Association has produced a ‘rules of engagement’ infographic setting out boundaries which you could use in your bio.

More info can be found here:

https://www.local.gov.uk/our-support/guidance-and-resources/civility-public-life-resources-councillors/handling-abuse-and-0

Deleting, purging or locking old social media accounts

There are countless examples of old social media accounts coming back to haunt those elected to office, so consider whether you need to set up a new account or remove messages (such as those that contain personal information) from your account before using it as part of your elected position.

If you wish to retain private accounts, for example, you may wish to review the settings on who is allowed to see or share your posts or to restrict access to your account

Setting up accounts securely

There are a number of things to bear in mind when setting up social media accounts. It is a good idea to use a unique and 'strong' password (which contains a combination of letters, numbers and symbols) to keep your account secure.

Two-step verification (2SV)

This is a way of checking that you are who you say you are when accessing online services. Passwords can be stolen by cyber criminals, but if you use two-step verification then anyone who has your password would still not be able to access your account.

You should find 2SV in the security settings of your account.

You should also use 2SV for your email account, as these can be used to reset passwords on other accounts you may have.

When you set this up you will be given the option to set up a second verification stage, which could be receiving a text message on your phone with a code to input. Some services will offer the opportunity to receive this code as a voice message.

Other examples of 2SV include use of authenticator apps such as Microsoft Authenticator and Google Authenticator. The advantages of using such apps are that you do not need a mobile signal and you do not have to wait for a text message to appear.

Some 2SV involves an email being sent to you, giving you the opportunity to use a code or click to confirm that you are who you say you are.

For further guidance on two-step verification, visit the National Cyber Security Centre website **here**.

Facebook

Facebook is one of the most popular social media platforms. If you choose this platform then you will need to set up a new 'campaign' account.

Ensure that any personal profile you may already have on the site is separate and that your name is chosen carefully or changed, as appropriate, to avoid constituents being able to find it.

You should also ensure any personal account has the highest possible privacy settings. You should also consider 'unfriending' people you haven't spoken to in a long time or potentially don't know well.

Set up a policy, which you can add to your bio or put into a pinned post which will appear at the top of your timeline, where you will explain how you intend to use the account. This would include, for example, when, how and who you will engage with and when you will block, to manage expectations.

If you keep direct messages (DMs) open then specifically state when and how often these are checked so people know not to follow up or use 'slow' responses against you. If you have this function enabled on a Facebook page you can set up an auto response.

Guidance on how to set up a Facebook account is available here: **https://help.instagram.com/454502981253053**.

X (formerly known as Twitter)

X, which was previously known as Twitter, offers users the chance to post either written, photo or video content, including links. Such posts are added to your timeline, which is accessible by any other user, and shown to your followers.

You can choose to follow a range of different accounts and can repost their content or reply to it as well.

You cannot edit posts once published, unless you subscribe and pay for an X Premium account. You can still delete posts, however.

X can be problematic in terms of the level of abuse and polarised views being expressed. Some users have left the platform as a result of this, preferring to use, for example, Instagram.

In terms of your security, you should also ensure your settings on X do not allow people to make video or audio calls as concerns have been expressed about this enabling people to then find out your location.

Think about how you want to use it. Do you want to 'broadcast' messages to followers? If so, then you need to know how to set things up to enable this.

We would recommend that you connect with allies/colleagues and agree to look out for each other, eg by sending encouraging messages or comments to colleagues if they are receiving negative posts.

For guidance on setting up an X account, visit **https://help.twitter.com/en/using-x/create-x-account.**

Instagram

Instagram is a free photo and video sharing social media app owned by Meta, which also owns Facebook. Content can be shared with followers or any users who look at your account, if it is public, or just with approved followers, if your account is private. There is also the option to create reels, which are videos available to non-followers, who could potentially become followers. This can be a good way to drive wider engagement with your posts.

For more information on setting up an Instagram account, visit **https://help.instagram.com/155940534568753.**

WhatsApp

WhatsApp is a free social media app owned by Meta. It offers encrypted and secure messaging between users or among group chats. It can also be used to make voice and video calls.

If you manage a group on WhatsApp you are able to delete inappropriate chats or media and you can also remove participants if they post abusive or offensive content.

More information about resources available to those running WhatsApp groups is available via **https://www.whatsapp.com/communities/learning.**

To find out how to get started with WhatsApp visit **https://faq.whatsapp.com/497209988909970.**

Scheduling posts

Scheduling important posts ahead of time can help if you want to take a break. This may depend on the platform you are using. However, do use these advisedly as scheduled tweets can become inappropriate or obvious. Scheduled posts can be very useful for holidays and closure days of your office, for example. Think about using these solely for things that are very unlikely to date or be controversial.

In an example of when scheduled posts can go wrong, we look at a Tweet published by Tesco's customer care team back in 2013.

The Tweet in question said: "It's sleepy time so we're off to hit the hay! See you at 8am for more."

Unfortunately for Tesco, however, in the time between the post being written and actually published, news had broken that Tesco had been selling products containing horse meat.

How to deal with online abuse

Any incidents of online abuse should, first and foremost, be reported to the police, where you are concerned for your safety, and to your colleagues and the platform in question.

There are options available within social media accounts which can also help when you are faced with online abuse. These include:

Blocking

Blocking a particular account will prevent that user from seeing your posts. Be aware, however, that some people will screenshot the message saying they are blocked and use it as a kind of trophy to share online. It may be better to mute such accounts, which prevents you from seeing their posts and interactions. For more on muting see below.

For advice on how to block accounts depending on the social media channel in question, visit the following links:

X (formerly Twitter) **https://help.twitter.com/en/using-x/blocking-and-unblocking-accounts**

Facebook **https://www.facebook.com/help/1000976436606344**

https://www.facebook.com/business/help/354716509063297

Instagram **https://help.instagram.com/454180787965921**

WhatsApp **https://faq.whatsapp.com/1142481766359885**

TikTok **https://support.tiktok.com/en/using-tiktok/followers-and-following/blocking-the-users**

Muting

Muting is an option that prevents you from getting that person's updates but without unfollowing or blocking them. The user will not know you have muted them.

X

Muting someone you do not follow means posts and interactions made by that particular user will not be visible to you. If, however, you mute someone you follow then replies and mentions will still appear, although their previous posts from before you muted them will be removed from your timeline.

Muting is preferable to blocking if the messages are annoying rather than abusive as some will use the block as a trophy by taking a screenshot and sharing the fact they have been blocked. However, if using muting liberally, do check replies

manually (i.e. not from mentions tab) as you won't be able to see the replies from here but others will be able to see the responses.

This may include abuse or disinformation. Mute-worthy accounts can escalate into block-worthy and this will need to be monitored.

When you click on a conversation then you will still see any replies or posts from the user you have muted. You can unmute them at any time. Muting does not prevent that user from sending you a direct message.

For more information on muting on the various social media platforms visit the following links:

X https://help.twitter.com/en/using-x/x-mute

Advanced muting options on X **https://help.twitter.com/en/using-x/advanced-x-mute-options**

Instagram https://help.instagram.com/469042960409432

Facebook https://www.facebook.com/help/408677896295618

https://faq.whatsapp.com/797069521522888

Untagging yourself

Untagging yourself from a concerning post will prevent you from receiving further notifications.

The links below contain guidance on doing this on the various platforms.

Facebook **https://www.facebook.com/help/140906109319589**

Instagram **https://help.instagram.com/178891742266091**

X **https://help.twitter.com/en/using-x/mentions-and-replies**

WhatsApp

How to exit and delete WhatsApp groups **https://faq.whatsapp.com/498814665492149**

Limiting replies (operating in broadcast mode)

On X, you can lock your account to enable only your followers to interact with you. You can also amend the settings on individual posts to prevent anyone from replying unless you have specifically mentioned them in the post.

Locked comments should be used advisedly as this has been seen to, for example, increase quote tweets (QTs) which can then spread the pile-on further than that which could transpire from allowing replies in the first instance. However, it can be useful, particularly for simple announcements.

Switching off notifications (or limiting to those you follow)

This can help you to control your use of and engagement with social media by removing what can potentially be a constant interruption to your flow. You have the choice to go into the individual social media accounts to check on any messages or comments, for example.

X

Mobile devices

This guidance includes how to enable and turn off notifications. It also includes advice on enabling or switching off push notifications, which are alerts sent to your mobile phone when you are not actively using the app.

https://help.twitter.com/en/managing-your-account/notifications-on-mobile-devices

Desktop

The following link gives guidance on both enabling and turning off notifications when using a desktop computer.

https://help.twitter.com/en/managing-your-account/enabling-web-and-browser-notifications

Facebook

Facebook states here that, while you cannot switch off all notifications, you can choose what you are notified about and how this will be done. This link also includes guidelines on how to switch off or customise notifications from a particular Facebook group.

https://www.facebook.com/help/269880466696699

Instagram

Guidance on switching off or customising notification settings on Instagram can be found here.

https://help.instagram.com/105448789880240

TikTok

Guidance on switching off or customising notification settings on TikTok can be found here.

https://support.tiktok.com/en/using-tiktok/messaging-and-notifications/notifications

WhatsApp

How to manage notifications on WhatsApp.

https://faq.whatsapp.com/797069521522888

Other social media

If you are using a social media app which is not covered here then please visit the app or website to obtain further guidance.

What to do if you experience online abuse

Reporting issues

If you see any concerning behaviour or abuse on social media then one of the things you should do is to report this to the social media platform in question. We have included links to the various platforms for when you wish to report any concerns you may have.

X

https://help.twitter.com/en/rules-and-policies/x-report-violation

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

Facebook

https://www.facebook.com/help/1380418588640631

Instagram

https://help.instagram.com/2922067214679225

https://help.instagram.com/489507671074566/?helpref=related_articles

TikTok

https://support.tiktok.com/en/safety-hc/report-a-problem

Messenger

https://www.facebook.com/help/messenger-app/1165699260192280

WhatsApp

Staying safe on WhatsApp

https://faq.whatsapp.com/1313491802751163/?helpref=hc_fnav

How to use social media safely

You should always set up dedicated professional social media accounts rather than using any existing personal accounts. If you do wish to retain an existing social media account on, for example, X (formerly Twitter), as you have already amassed a number of followers, then there are ways to delete previous posts.

For more information on deleting posts manually via the X app, visit **https://help.twitter.com/en/using-x/delete-posts.** They can only be deleted individually via the app itself.

Always use long and unique passwords and make sure they are different for each account. They should be 16 characters or more and should not include any personal details which could be easy for hackers to guess. You could use a password manager to help with coming up with passwords.

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

Be cautious about any emails which have come from an account you do not know or which may even, at first glance, look like they have come from a particular company or organisation. They could be what are called phishing emails.

Such phishing emails are designed to look like they have come from a contact or a genuine company or organisation. But when you look closely at the email address, for example, you can see it is not a genuine email from a particular company.

Sometimes such phishing emails or messages will be designed to invoke an urgent response from the recipient. Those sending such emails will try to get past your usual defences by making you react quickly and panic by using phrases such as 'security alert'.

Phishing emails could, for example, claim there is a security alert on your account. They will often have typos or grammatical and spelling errors too. Always check and, if in doubt, do not open or respond to such emails and make sure you report any such activity.

This 'check a website' service, on the Government-supported website, Get Safe Online enables you to check if a website is genuine.

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

Ensure you regularly update your apps to ensure they have the latest fixes and security updates.

What to do if you experience harassment

If you feel threatened by online abuse then you should notify police. You should also notify the appropriate council officers, along with your party colleagues and the relevant social media platform.

If you report a concern to a social media platform then it is up to that platform to take action.

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/.**

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

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.

General guidance on staying safe online

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

You can check if your email has been involved in a data breach by going to the following site - **https://haveibeenpwned.com/**

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 you update apps 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 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

Further resources on the Local Government Association website

Handling online abuse and intimidation national webinar presentation

Councillors' guide to handling harassment, abuse and intimidation

Social media guidance for councillors

Digital citizenship: support and resources for councillors

Debate Not Hate Campaign Resources

Seven principles for safer canvassing

Further reading

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/

The Local Government Association

https://www.local.gov.uk/our-support/communications-and-community-engagement/social-media-guidance-councillors

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

https://docs.google.com/document/d/1iftaofIxjGqrMj4kSiua_G3Ih-E_wfR6onmemLR9rL0/edit#heading=h.xubrbixchv8m

The National Association of Local Councils

https://www.nalc.gov.uk/our-work/civility-and-respect-project#social-media-guide

Welsh Local Government Association guide

https://www.wlga.wales/SharedFiles/Download.aspx?pageid=62&mid=665&fileid=344

National Cyber Security Centre

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

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

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.