HM Government

Candidate security guidance for local elections

May 2025

Contents of this guidance

All of this and further information can be found on the Candidate Security Guidance Page on GOV.UK - your one-stop-shop for candidate security information.

Candidates can also contact their political party (if you are a candidate on behalf of one) or their Returning Officer.

---

1. Five ways to improve your personal security today:

1. **Watch this protective security video from the NPSA and police**
2. **Understand when behaviour goes beyond political debate and may be unlawful**
3. **Take up the full cyber security offer from the National Cyber Security Centre**
4. **Read more detailed cyber security guidance for high-risk individuals**
5. **Improve your information security and understand what you can do if you're affected by online disinformation.**

2. Further information on your personal security and policing arrangements

During previous election periods, some candidates have been exposed to unacceptable harassment or intimidation. This can take place in person or online and may also be directed at a candidate's family, friends, and colleagues.

It is vital that you call 999 when harassment or abuse escalates in the following way:

HM Government

- A 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 weapons skills.
- If the person releases personal information about you not already in the public domain.

The Candidate Security Guidance Collection page on GOV.UK includes protective security guidance from the National Protective Security Authority (NPSA) for election candidates.

Government has issued a video which highlights where candidates can access relevant security advice and guidance that may be helpful to you during an election period and beyond. There are three key things candidates need to do: "**be alert, plan ahead, and know what to do"**

Primary responsibility for security during the election lies with your local police force. If you're at risk of harm or in immediate danger, call the police on 999. If a crime has been committed, contact your local police on 101 or via police.uk.

The May 2025 local elections will be the first elections where Operation Ford will be up and running in police forces. Under Operation Ford, every police force has at least one Force Elected Official Advisor (FEOA). The FEOA is a police officer dedicated to the safety and security of elected representatives (local councillors, mayors, police and crime commissioners) and candidates for those roles.

After close of nominations, FEOAs will make contact with returning officers to offer essential personal security briefing to all candidates.

FEOAs are not a route to report incidents or crimes, given as individuals they are not on duty 24/7. As above, candidates and locally elected representatives should report incidents via 999 if a crime is in process or there is an immediate threat to safety, or via 101 or police.uk if a crime has been committed, so that incidents can be triaged appropriately by police control rooms. Candidates should flag their role so that the incident can be logged as an Operation Ford incident.

An Operation Ford incident is an act committed against a serving locally elected representatives including local councillors, mayors, police & crime commissioners, or candidates for those roles, where it is reasonable to believe that the act has been committed with the intention of intimidating or harassing the elected representative or candidate in connection with his/her official position or potential future position.

3. Further information on your cyber security

Candidates for elected positions may find themselves at higher risk of targeted attacks online. Cyber attacks can take many forms including hacking (when

HM Government

unauthorised access to accounts may lead to the theft of private information), phishing (scam emails or text messages that contain links to websites which may contain malware, or may trick users into revealing sensitive information), spear-phishing (phishing targeting particular individuals, where the email is designed to look like it's from a trusted or known person) and impersonation (where an attacker creates a fake account to impersonate you or your contacts). Additional threats include doxxing (release of personal information online) and spam flooding (unsolicited use of email address to register for spam mail).

The Candidate Security Guidance Collection page on GOV.UK contains guidance to help you improve your personal cyber resilience, published by the National Cyber Security Centre (NCSC). This includes:

- Cyber Security Guidance for high-risk individuals – this includes candidates for elected positions and elected representatives, who are often more visible figures than the general public.
- Guidance for candidates setting up their own personal email/web domains to support their campaigns, to make them more secure against cyber attacks.
- How to sign up for a range of Individual Cyber Defence (ICD) services for people at higher risk of being targeted online – including elected representatives and candidates for elected roles – to ensure they can better protect personal accounts and devices from cyber-attacks. These include:
    - NCSC Personal Account Registration Service (PARS): enables election candidates to register their details to allow the NCSC to notify you if the NCSC becomes aware of a cyber incident impacting a personal account. It also allows you to sign up for additional protections from Industry partners that aren't publicly available.
    - NCSC Personal Internet Protection (PIP): an app which provides an extra layer of security on personal devices to reduce the risk from clicking on known malicious links in emails or messaging apps.

To sign up for these services, please email the NCSC on individualsupport@ncsc.gov.uk

4. Further information on your online security

Your online presence as a candidate may give rise to risks that could be heightened during an election period. Generative artificial intelligence (AI) presents new risks, such as deepfakes and AI-generated media (video, image or audio) that may imitate individuals. These sit alongside, and potentially exacerbate, existing risks like disinformation or online abuse and harassment.

The Candidate Security Guidance Collection page on GOV.UK contains key information including from the police and Electoral Commission to help keep you safe online.

HM Government

AI generated disinformation

Generative AI is software that can create high quality audio or visual 'fake content', including text, images and video. It has been possible to create or doctor images for a long time; what's changed is the ease with which fake content can now be created (and how quickly it can be shared online) allowing attackers to spread disinformation. 'Deepfakes' are a type of AI-generated fake content, consisting of audio or visual content that misrepresents real people as doing or saying something that they did not actually do or say.

If you are affected by disinformation or generative AI content:

- **Report details to the platform** – the candidate security collection page on GOV.UK has links to report content to X (formerly Twitter), Meta (Facebook, Instagram, WhatsApp, and Threads), Google (YouTube) and TikTok.
- **Report details to your political party,** if you are a member of one, who will be able to offer support and advise on any channels in place to escalate cases to platforms or the police.
- **Think before you respond** to any reports of disinformation. This may inadvertently amplify the suspected disinformation and could make the matter worse. If an official response is required, use official channels and avoid referencing the disinformation.
- **Call 999** if you feel a threat or danger is immediate, or 101 if you think a crime has been committed.

Finally, the personal security guidance outlined at the start of this document contains guidance on staying safe online and when to report incidents to the police.