HM Government

Candidate security guidance for local elections in England and the Senedd election in Wales, May 2026

Note this guidance is intended for distribution to candidates for local elections in England and the Senedd election in Wales in May 2026. Police Scotland will issue guidance to candidates standing for election to the Scottish Parliament.

Contents of this guidance

1. Five ways to improve your personal, online and cyber security today
2. Your personal security and policing arrangements
3. Your cyber security
4. Your online security
5. Have your say

All of this and further information is contained on the GOV.UK candidate security guidance collection page - 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.

Important: If you, or a member of your staff believe you have been the victim of a crime, either in person, or online, report this immediately to your local police, either by 999 or filing a report on police.uk.

HM Government

1. Five ways to improve your personal, online and cyber security today:

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

2. Your personal security and policing arrangements

Unfortunately, harassment and intimidation is an issue for many candidates. It can take place in person or online and may be directed at your family, friends or staff.

It is vital that you call 999 when abuse escalates in the following ways:

- 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 both access to weapons and weapons skills.
- If the person releases personal information about you which is not already public.

The Candidate Security Guidance Collection page on GOV.UK includes protective security guidance from the National Protective Security Authority (NPSA) for election candidates, including guidance on protecting democratic institutions from espionage and foreign interference.

HMG has issued a video which may be helpful to you during an election period, focusing on three key things "**be alert, plan ahead, and know what to do".**

HM Government

Policing arrangements

If you're at risk of harm or in immediate danger, call the police on 999. If a crime has been committed, contact the police on 101 or via police.uk.

Under Operation Ford, every police force has at least one Force Elected Official Advisor (FEOA) in place. The FEOA is a police officer dedicated to the safety and security of elected representatives (MPs, MSPs, MSs, local councillors, elected mayors, and police and crime commissioners) and candidates for those roles.

After close of nominations, FEOAs will contact returning officers to request candidate contact details to offer essential personal security briefing.

FEOAs are **not a route to report incidents or crimes.** You 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 you think a crime has been committed, so that incidents can be triaged by police control rooms. When reporting to the police, candidates should flag their role so that Operation Ford incidents can be recorded. An Operation Ford incident is any act against a serving local elected official or candidate, reasonably believed to be intended to intimidate or harass them in connection with their role. Crime or incidents not related to their elected office or candidacy are not Operation Ford incidents and will be treated in the same manner as crime against a private individual.

3. Your cyber security

Candidates for elected positions may find themselves at higher risk of targeted cyber-attacks, which can take many forms including:

- **Hacking**: unauthorised access to your accounts, potentially leading to the theft of your private information;
- **Phishing**: scam emails or text messages that contain links to websites which may contain malware, or may trick you into revealing sensitive information;
- **Spear-phishing**: phishing targeting you specifically, where the email is designed to look like it's from someone you trust;
- **Impersonation**: where an attacker creates a fake account to impersonate you or your contacts;
- **Doxxing**: release of your personal information online;
- **Spam flooding**: unsolicited use of your email to register for spam mail.

As a candidate, you can sign up for a range of Individual Cyber Defence (ICD) services from the National Cyber Security Centre (NCSC) to protect your personal accounts and devices from cyber-attack, including:

HM Government

- NCSC Personal Account Registration Service (PARS): enables the NCSC to notify you if the NCSC becomes aware of a cyber incident impacting your personal accounts. It also allows you to sign up for additional protections from Industry partners that aren't publicly available.
- NCSC Personal Internet Protection: to provide an extra layer of security on your personal devices to reduce the risk from clicking on malicious links received via email or messaging apps such as WhatsApp or Signal.

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

The Candidate Security Guidance Collection page on GOV.UK contains further NCSC guidance to help you improve your personal cyber resilience, including:

- Cyber security guidance for high-risk individuals – including candidates
- Guidance to ensure your personal email and web domains are more secure against cyber attack.

4. Your online security

Your online presence and profile as a candidate for elected office could unfortunately make you the target of online mis and disinformation, potentially including AI-generated content such as deepfakes.

The candidate security guidance collection page on GOV.UK contains guidance from the police and Electoral Commission to help keep you safe online.

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

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 shared, 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 relevant platform** – the candidate security collection page on GOV.UK contains links to report content to X, Meta (Facebook, Instagram, WhatsApp, and Threads), Google (YouTube) and TikTok.

HM Government

- **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.

5. Have your say

In June your Returning Officer and/or party will send you a link to a questionnaire about the usefulness and scope of this guidance. Your feedback is invaluable for future improvements.