I am a candidate, how can I improve my security?

1. **Watch this protective security video**
2. **Take up the full cyber security offer available to me from the National Cyber Security Centre**
3. **Know how to improve your information security and understand where to go if you're affected by online disinformation.**

You may also want to…

Read more detailed cyber security guidance for high-risk individuals

Understand when behaviour goes beyond political debate and may be unlawful

Find out more about social media (both securing your accounts and reporting content)

For more guidance, please go to the Candidate Security Guidance Page - your one stop shop for security guidance. The following sections also set out some of the help that is available, and steps candidates can take. More detailed guidance is available through the links provided. You can also contact your political party (if you are a candidate on behalf of one), your Returning Officer or your *Operation Bridger Single Point of Contact (SPoC) for further information.

**Operation Bridger is the network of police officers who work with election candidates in the General Election on their safety, and there is one for every police force. The SPoC for your constituency will be making contact with you to introduce themselves, explain more about their role and offer you a security briefing; you will see them referred to throughout this briefing note.*

Personal ("protective") security

The 'Candidate Security Guidance Collection' GOV.UK includes protective security guidance from the National Protective Security Authority for election candidates.

- HMG has also 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 that you as candidates need to do: “be alert, plan ahead, and know what to do”.
- Primary responsibility for security during the general election lies with your local police force.
- If you’re at risk of harm or in immediate danger, phone the police on 999. If a crime has been committed, please contact your local police on 101.
- You can also contact your local Operation Bridger SPoC to relay concerns or issues.
- Through Operation Bridger every force will offer a security briefing to all General Election candidates in a constituency in their area. Briefings are nationally led but include local threat information around protest, public order and provide details of local Police contacts. We encourage all candidates to take up this offer.
- Bridger SPoCs are reaching out to all Returning Officers to identify themselves. This means you can find the details of your Bridger SPoC through your Returning Officer.
- In addition Bridger SpoCs will be in touch with candidates directly to identify themselves and provide further information on the support available, including the offer of a security briefing.
- We encourage you to remain in regular contact with the Bridger point of contact in your local force throughout the campaign.
- Dependent on fulfilling criteria and scope, and supplementary to policing activity, the Home Office can also provide private security. This ranges from accredited door supervisors to additional private security provision, available dependent on risk.
- The Home Office can also provide Situational Awareness Training and Cyber Security Awareness Training beyond that provided by policing.
- The Home Office will consider requests for security on a case-by-case basis, judging each request on its own merits. To request security, please email HomeOfficeprivatesecurity@homeoffice.gov.uk.
- Through the Local Communities Fund, Police in England and Wales are also able to fund additional patrolling in areas that might benefit from a policing focus. Your Returning Officer will be working closely with them on the policing arrangements for the election.

Cyber security

The National Cyber Security Centre (NCSC) has published a range of guidance to help counter the cyber threat to our democratic processes. This includes dedicated

advice for individuals at higher risk of being targeted, such as election candidates and officials, and for organisations such as political parties and local authorities.

- The 'Candidate Security Guidance Collection''GOV.UK page includes Cyber Security Guidance for high risk individuals issued by the National Cyber Security Centre (NCSC)
- NCSC has also developed a range of **Individual Cyber Defence (ICD)** services for people at higher risk of being targeted online to ensure they can better protect their 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 alert individuals if the NCSC becomes aware of a cyber incident impacting a personal account. It also highlights additional security features from industry that can further protect personal accounts.
- **NCSC Personal Internet Protection (PIP)**: An opt-in service that provides an extra layer of security on personal devices to reduce the risk from spear-phishing. When you browse the internet or use mobile apps, PIP checks the domain against a known malicious list. If the domain is on the block list, your device will show a warning. If your device is already infected with malware, PIP will block outgoing traffic to known malicious IP addresses and domains, to prevent you from accessing websites that host or link to malware and other cyber threats. To sign up for these services, please email the NCSC on candidates2024@ncsc.gov.uk
- The NCSC also remains committed in supporting the cyber resilience of Party IT networks and offer a range of free **Active Cyber Defence** services which we encourage all parties to take advantage of. The NCSC is happy to assist Party IT leads with getting these setup - please contact individualsupport@ncsc.gov.uk
- The NCSC also strongly encourages all political parties to have an NCSC-approved **Cyber Incident Response** (CIR) company on retainer to assist in the event of an incident . The CIR framework meets NCSC rigorous standards for a high-quality response service. Scheme members can deliver a full investigation along with recommendations on how to prevent a cyber incident happening again

Information security

Your online presence as a candidate may give rise to risks that could be heightened during the election period. The recent rise of 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.

During the election, there are a range of resources available to you as candidates to help keep you safe online and below is key information to support you. Your local Returning Officer, police forces and Electoral Commission materials can help you throughout the election period.

Online Harassment/Abuse

During previous election periods, some candidates were exposed to unacceptable levels of online harassment or intimidation. Harassment and intimidation may also be directed at a candidate's family, friends, and co-workers.

It is vital that you contact your local police force (by dialling 999) when harassment or abuse escalates in the following way:

- 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.
- You can also contact your local Operation Bridger SPoC to relay concerns or issues.

If you wish to report content to social media platforms yourself you can find details on how to report content to X (formerly Twitter), Meta (Facebook, Instagram, WhatsApp, and Threads), Google (YouTube) and TikTok on Gov.uk. We would recommend you familiarise yourself with social media platforms' policies and processes regarding disinformation and AI-generated media to ensure you understand what is permitted on their sites and how to report content.

Further guidance for candidates on online harassment and abuse can be found in the Joint Police Guidance for candidates in elections. This guidance provides information for candidates on the following types of harassment and abuse:

- Communications, on or offline, which contain abusive or threatening language.
- Repeated unwanted contact that may constitute harassment or stalking.
- Racial, homophobic, misogynistic or other discriminatory abuse or threats.
- Fixation on you or an issue associated with your campaign.

AI generated disinformation

Generative AI is software that can create high quality ‘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. The most prevalent types of content created by generative AI tools (and some high-profile examples) are included below.

- **Fake text:** Text generation tools can be used to quickly and cheaply create unique content to post on social media platforms.
- **Fake images**: Image generation tools can be used to produce fake images intended to mislead the voting public. These could feature candidates, election procedures, the trustworthiness of election officials, and other issues that may affect voter behaviour or turnout.
- **Fake videos** (deepfakes): Video tools can be use create convincing ‘deepfakes’ that purportedly feature real individuals, which may be used to mislead the public about candidates or the election, and to provide a seemingly trustworthy source for disinformation campaigns
- **Fake audio**: Like video, audio deepfakes can provide convincing speech from a well-known individual, which may be used for disinformation campaigns.

If you are affected by disinformation or generative AI content:

- Report details to the relevant platform – there are details on Gov.uk. above on how to contact X (formerly Twitter), Meta (Facebook, Instagram, WhatsApp, and Threads), Google (YouTube) and TikTok.
- Report this to your political party, who should be able to offer support and have relevant comms 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.
- If you feel a threat or danger is immediate, you should call 999.

We have also previously seen 'prank calls' made to prominent individuals, the content of which is then distributed online. The objective is often to embarrass or obtain private views that are then made public. When agreeing to requests for telephone conversations or online interviews, candidates and their teams may want to do due diligence in advance to make sure the caller or emailer is genuine and are who they say they are.