
15 WHITEHALL, LONDON, SW1A 2DD. 020 3878 3955
hello@demos.co.uk, www.demos.co.uk

EPISTEMIC SECURITY BRIEFING

THE ELECTIONS BILL

Background

In an era of democratic emergency, [our epistemic security](#) – the resilience of the UK’s information supply chains that our democracy depends on – is under threat.

Blaise Metreweli, Chief of MI6, supports this, [claiming in a recent speech](#) that “our world is more dangerous and contested now than it has been for decades.” Demos is convening leading thinkers to tackle these wide-ranging vulnerabilities threatening the information environment, we host the [Epistemic Security Network](#) (ESN) to do exactly that.

Within the ESN, Demos convenes the Information Crisis Coalition – a partnership between Full Fact, Transparency International, the UK Anti-Corruption Coalition and the Online Safety Act Network – which focuses specifically on strengthening resilience to information crises, including during election periods.

This briefing sets out the Coalition’s current recommendations on the upcoming Elections Bill and wider policy framework which can be used as an opportunity to safeguard future elections from epistemic risks, such as the spread of false or unreliable information and the harassment of MPs and candidates.

About the Elections Bill

Ahead of the publication of the Elections Bill, our understanding of its contents is currently shaped by the [Elections Strategy](#) published in July 2025. As a result, this briefing and our

recommendations will be replaced with a revised version once the text of the Bill has been published.

The Elections Strategy explicitly states that “our own democracy is being threatened by misinformation”, and yet it only goes some way towards addressing the risks that the UK’s electoral system faces. The final Elections Bill needs to go much further to avoid missing this opportunity to tackle new and emergent threats and safeguard our democracy.

While we appreciate that the Elections Strategy pays attention to harassment and intimidation towards candidates, digital political advertising, and campaign finance, we believe much greater detail is needed on these issues. Moreover, the eventual Bill must go further than the current Strategy when it comes to addressing the risk of false and unreliable information during elections.

The current Strategy does not address the role of digital platforms in electoral mis- and disinformation, including deepfakes of candidates and MPs. Nor does it address the potential for crisis situations to arise due to such content, which could cast doubt on the legitimacy of an election. And while it does propose reforms to political advertising and a new Code of Conduct for digital campaigning, the Strategy’s proposals do not specifically address the risk that digital political advertising could be used to spread false or unreliable information. Nor does the Strategy address the need to reform campaign spending limits to address runaway spending on digital ads.

The Strategy features similar gaps when it comes to conduct during elections and the Electoral Commission. It does not provide significant detail on the Government’s intended campaigning Codes of Conduct, nor the framework of oversight and compliance for this voluntary code for parties.¹ It also lacks detail on measures to address online abuse directed at candidates and MPs.

Recommendations for the Elections Bill

The following sections summarise our recommendations for provisions to be included in the Elections Bill - or where the Bill provides an opportunity to advance vital non-legislative reforms. Our key recommendations are:

1. Introduce systems to reduce online threats and abuse against candidates
2. Publish guidance which clarifies the law on electoral information incidents, including deepfakes of candidates and MPs
3. Establish further regulation and transparency in political advertising
4. Reduce spending limits at elections to address runaway spending on social media
5. Increased the Electoral Commission’s investigative powers
6. Establish a public protocol for election information incidents

¹ On the voluntary Code of Conduct for digital campaigning.

<https://questions-statements.parliament.uk/written-questions/detail/2025-10-27/85163>

1. Systems to reduce online threats and abuse against candidates

The UK has seen a rise in violent and threatening online behaviour aimed at election candidates. [Research by the Electoral Commission](#) found that over half (55%) of candidates that responded to its survey “felt that they had some kind of problem with harassment, intimidation, or abuse” during the 2024 General Election. 70% of responding candidates said they had experienced at least one incident of abuse. Of candidates that had experienced abuse, 65% said this had come from online sources.” Female respondents and respondents from ethnic minority backgrounds were more likely to report having experienced serious abuse.” The Speaker’s Conference, launched to examine and recommend routes to tackling this issue, provided a number of robust recommendations for offline threats in its [first report](#). The Conference’s [second report](#) specifically addressed the significant role that social media plays in abuse and covered steps which platforms should take to reduce such abuse, such as by providing candidates with named points of contact for support.

The Online Safety Act Network has developed proposals for enhanced civil regulation of elections and online media to assess and mitigate the risks to candidates and other election participants. Their proposed Elections Code would require the Electoral Commission and the National Police Chiefs Council to work with Ofcom and platforms to assess the risks of harm to victims and then put in place systems under the Online Safety Act (OSA) regime to mitigate those risks. The Speaker’s Conference second report [endorses this proposal](#) and recommends that it should be included in the Election Bill.

Recommendations

The Elections Bill should amend the OSA to require digital platforms to extend their protections and support for electoral candidates. As [suggested by the OSA Network](#), these requirements could be introduced through the Elections Bill via an amendment to the OSA requiring Ofcom to produce a code of practice. The OSA amendment should require Ofcom to lead on addressing harms arising from the operation of online platforms during elections, in consultation with the Electoral Commission and NPCC. Ofcom would produce a Code of Practice describing measures for platforms to reduce harms such as the abuse and harassment of or threats directed towards elected representatives, candidates, party campaigners and election officials.

While the OSA Network is currently working with experts on an updated draft Elections Code for publication, indicative requirements for platforms should include:

- A duty to assess and mitigate the risk of online threats and abuse towards candidates and MPs.
- Transparency and data access duties regarding hate and harassment directed at

candidates, including data on how content directed at candidates has been moderated.

- Changes to recommendation systems to reduce the amplification of hateful and harassing content directed at candidates.
- Requirements to communicate promptly and clearly with candidates.
- Requirements to offer candidates a high standard of customer service, such as a human customer service representative via a hotline.
- Requirements to provide candidates with tools to limit their exposure to hateful and harassing content, such as the ability to block all direct messages (DMs) and keyword based filters.

For more on this recommendation, see the OSA Network's briefing [here](#).

2. Publish guidance which clarifies the law on electoral information incidents, including deepfakes of candidates and MPs

While the UK has so far [not seen a major incident](#) involving the spread of false or misleading information which disrupt an election, there have been several concerning cases which could be a sign of things to come. In October 2025, a [deepfake video of the Conservative MP George Freeman](#) gained public attention, in which a falsified likeness of Freeman claimed that he intended to defect to another party. Meanwhile in October 2023, [deepfake audio of Prime Minister Keir Starmer](#) went viral and has re-emerged at regular intervals since. Looking beyond the UK, Ireland's recent presidential election was [disrupted by a viral AI-generated video](#) which depicted frontrunner Catherine Connolly saying she would exit the race. With the emergence of [AI video creation platforms](#) that allow ordinary users to create convincing deepfakes of other people, there is a serious risk that deepfake content could be used to mislead voters in future elections.

Yet there are ambiguities and gaps in the law surrounding deepfakes and AI-generated videos targeting election candidates and MPs. The laws which set out election offences do not explicitly or specifically address digital communications, deepfakes or other AI-generated content – resulting in ambiguity about the extent to which these harms are covered by election law. Meanwhile, the OSA does not address elections specifically. The relevant laws and their limitations include:

- Section 106 of the Representation of the People Act 1983 (RPA), which criminalises the act of making false statements made about the personal character or conduct of candidates and MPs.
- Section 8 of the Elections Act 2022 (EA), which amended the RPA to criminalise the use of violence, threats or reputational damage to influence voters' decisions.²

² The Elections Act 2022 inserted this offence into the RPA as Section 114a.

- Section 179 of the Online Safety Act 2023 (OSA), which makes it a criminal offence for a person to spread information they know is false with the intent of causing serious harm to an audience, and other OSA Priority Offences.³

All three laws may be interpreted as covering deepfakes and AI-generated videos targeting candidates and MPs during elections. But none of them state this specifically or explicitly: neither the RPA nor the EA explicitly address digital communications or deepfakes, while the relevant parts of the OSA do not specifically address elections. Clarifying these ambiguities could aid prosecutors, campaigners, and targets of deepfakes: as [highlighted by the Electoral Commission](#), the lack of explicit references to digital communication or deepfakes in the RPA may make it harder for law enforcement to identify appropriate cases and leave survivors unaware of the potential legal remedies available to them.

There is also some ambiguity about the extent to which the OSA places duties on platforms to take steps to mitigate the risk of the content which violates the RPA and EA, due to the way that duties work for relevant non-priority offences. Because of the 'safe harbour' clause, platforms are only required to take the preventative measures set out in Ofcom's Codes of Practice. While there are some general measures applying to all relevant offences, the Codes focus on measures to tackle priority offences in Schedules 5- 7 of the OSA. The S106 and EA S8/RPA S114A offences are not priority offences in the OSA, so platforms are not required to take preventative measures in relation to them. In addition, Ofcom has not identified them in its Illegal Content Judgments Guidance, so the scope and applicability of these offences might not be apparent to services. The [government has suggested](#) that it is reviewing the extent to which generative AI is covered by the OSA, though this review may focus on text-based chatbots rather than deepfakes or other AI imagery.

Gaps and ambiguity can lead to barriers in enforcement. During the 2024 General Election, UK police [considered 90 alleged offences under section 106](#), but most cases led to no further action and no allegations resulted in a prosecution. The Electoral Commission has written that police and prosecutors could be aided if it was made clear that "the scope of [RPA Section 106] does cover digitally manipulated false statements of fact about the personal character or conduct of a candidate." As the Commission also noted, Section 106 specifically applies to false statements of fact about the personal character or conduct of a candidate – not their political views, conduct in office, or other significant subjects which may be the targets of election disinformation. Meanwhile, the [Director of Public Prosecution](#) has highlighted that the RPA's wording sets a high bar for prosecuting false statements offence because it allows for a defence that a person had "reasonable grounds for believing, and did believe, that statement to be true."

³ The Online Safety Act does cover deepfakes of candidates and MPs if these count as sexually explicit images under its provisions criminalising the creation and sharing of Non-Consensual Intimate Images (OSA Section 188), as well as specific situations where deepfakes meet the criteria for another of the OSA's Priority Offences.

Moreover, Ofcom has consulted on [guidance for platforms](#) to implement crisis protocols in accordance with the OSA. But because the OSA does not specifically address elections as a high-risk context, tackle collective harms to democracy, or include the above-referenced offences as priority offences in the OSA, the proposed crisis protocols do not contain measures that are tailored to elections. [Demos](#), the [OSA Network](#) and [Full Fact](#) have each raised these concerns in more detail via their respective submissions.

The government and Ofcom should publish guidance to clarify how these laws relate to deepfakes and similar AI-generated material, including video and images, targeting election candidates and MPs. Such guidance will help provide more consistency in how the law is applied and reduce the risk of misinterpretations. It is vital for there to be more fairness and consistency in how these offences are interpreted and prosecuted. By identifying how these laws relate to digital services, new guidance may be a means to ensure that platforms take appropriate action.

In the context of these gaps in the OSA's provision and legal uncertainties around the status of existing elections offences, our recommendations are designed to extend platforms' risk assessment obligations to address and therefore proactively mitigate the specific risks posed to elections, including deepfakes of candidates and MPs.

Recommendations

To accompany the Elections Bill, the government and Ofcom should publish guidance to clarify how existing laws relate to false claims online, deepfakes, and AI-generated videos targeting election candidates, MPs and voters.

For the government: publish guidance as a matter of urgency to give clarity to the public, platforms and law enforcement that clarifies how the RPA Section 106 and EA Section 8 apply to digital contexts, including deepfakes and AI-generated content. This should make it clear that these offences do apply to online communications and should set expectations about the standard of evidence required. If the government determines that there are indeed gaps, then such gaps should be closed during the passage of the Bill.

For Ofcom: publish guidance which addresses how the OSA relates to existing election offences and elections more broadly:

- (1) Guidance which clarifies the status of the RPA Section 106 and EA Section 8 under the OSA. This should specify platforms' duties to address content which violates these laws.
- (2) Guidance which specifically addresses how the False Communications Offence and other Priority Offences under the OSA should be addressed during elections.

This should include how these offences apply to deepfakes and AI-generated content of candidates and MPs.

To share examples of deepfakes, please get in touch at: deepfakes@demos.co.uk

3. Establish further regulation and transparency in political advertising

Digital political advertising continues to lack transparency, is prone to being used to spread false or misleading information, and remains open to being manipulated by foreign interests. The Government's [Elections Strategy](#) includes proposals to reform aspects of the digital campaigning regime but does not go far enough.

Digital imprint rules require electoral campaigners that produce campaigning material to include the name and address of the promoter of the material, as well as the name and address of any person on behalf of whom the material is being published. This applies to digital political advertising as well as in-person material. The Government's Elections Strategy proposes to extend these rules "by requiring campaigning material promoted by or on behalf of certain political entities to include information about party affiliation – or a statement of independence where applicable." The stated aim is to help voters "better understand the origin and intent of the material they see, enabling them to make political choices with greater confidence."

We are calling for the Elections Bill to go beyond these proposed measures by introducing additional regulation and transparency requirements for political advertising. These measures are needed to ensure that digital political advertising is transparent, is not used as a vehicle for misinformation, and is not open to manipulation by wealthy foreign interests.

Recommendations

The Elections Bill should establish a public repository for all paid-for digital political advertising, based on the definition of paid-for political advertising in the Elections Act 2022. Large online platforms and search engines should be required to make prescribed information available in the repository in as close to real-time as possible, and no later than 72 hours after the advert is published. Ofcom should be given sufficient resources to build and maintain the public repository, and should consult the Electoral Commission, Information Commissioner's Office (ICO), and civil society on the transparency notices.

The material should be transferred to the National Archives and made publicly available, to avoid historic barriers to transparency and scrutiny.

The Bill should also establish a regulatory framework to prevent mis- and disinformation in political advertising. It should establish a regulatory committee on political advertising, including relevant experts from the ASA, Electoral Commission, Ofcom, the UK Statistics Authority and the ICO. The committee should have powers to adjudicate breaches of a new code of practice. The regulators should work with political parties to develop a code of practice on political adverts. This should cover clearly misleading statements of fact in all political advertising, not just commercial marketing, to reflect the wider regulatory framework for advertising. It should also cover egregious misstatements of fact about an electoral process.

Finally, the Bill should introduce restrictions on overseas spending on political advertising in the UK at all times, rather than just during election campaign periods

For more details on these proposals, we recommend reading [Full Fact's briefing on the Elections Strategy](#).

4. Lower spending limits at elections to reduce the funding arms race and reliance on wealthy donors

Spending on digital election campaigning via social media platforms has [grown greatly in recent years](#). An [analysis](#) of political advertising spending during the 2019 General Election suggested that over half went towards ads on Facebook, Google, Twitter and Snapchat – an “exponential rise” from just under a quarter in 2015. Yet the [rules governing political spending](#) during elections remain complex and, at times, ambiguous. As a result, there is a risk that spending on social media platforms will continue to rise with each election. The Government’s Elections Strategy does not address this risk and lacks proposals on political spending entirely.

Recommendation

The Elections Bill should reduce a campaign spending limits to a ceiling of £16.1 million. These rules should also cover campaign staff costs, which the law currently excludes from the limits for political parties yet not those for non-party campaigns. At the very least, the government should return candidate spending limits to pre-2023 levels.

For more details on these proposals, see Transparency International’s [briefing on political spending](#).

5. Increased investigative powers for the Electoral Commission

The Government's Elections Strategy includes measures to increase the Electoral Commission's enforcement investigative powers: it proposes increasing the maximum fine for an offence from £20,000 to £500,000, and sets out additional express powers for the Commission to share information with some regulators and enforcement authorities in certain circumstances.

However, these proposals do not address the fact that, unlike the Information Commissioner, the Electoral Commission does not have the power to obtain information outside of a formal investigation. As a result, the Commission cannot request information from social media platforms in real-time during an election information incident. The Commission has [previously said](#) that this lack of powers has limited its ability to act quickly. Such gaps in powers will also significantly undermine the Commission's new statutory information-sharing gateway.⁴

Recommendation

The Elections Bill should grant the Electoral Commission the power to obtain information outside of a formal investigation, including from online platforms. The Commission would then be better positioned to monitor and enforce rules on campaign spending and the attempts to influence voters.

For more details on these proposals, see [Full Fact's briefing on the Elections Strategy](#) and the [UK Anti-Corruption Coalition's](#) briefing on increased powers needed by the Electoral Commission.

6. Establish a public protocol for election information incidents

Unlike our close allies, [such as Canada](#), the UK lacks a democratically accountable mechanism for the Government to notify the public about information incidents during election periods. An information incident could include situations such as a deepfake of a candidate that misleads voters on their views or an online campaign seeds rumours that the election has been cancelled. Without transparency about measures to respond to such

⁴ See Recommendations 5 and 6 from this briefing by the UK Anti-Corruption Coalition on Electoral Commission's powers for more detail. <https://www.spotlightcorruption.org/wp-content/uploads/2024/05/Key-Electoral-Reforms-Recommended-by-Independent-Experts-public-version.pdf>

incidents, government actions in response to an incident could be perceived to limit voters' freedom of expression, fuel further distrust and thus undermine an election's perceived legitimacy.

While we understand that general crisis protocols may exist, these are neither transparent nor accountable. It is our understanding that the government's [Election Cell](#) is primarily responsible for monitoring information incidents during an election, with support from the National Cyber Security Centre, the National Security Online Information Team, and the Joint Election Security Preparedness Unit. We understand that these teams do operate according to internal procedures for responding to election incidents. However, these procedures have not been made public and, in fact, the government has stated it has no plans to introduce such a public protocol when these internal systems exist.⁵ As part of any public disclosure of the government's procedures for responding to information incidents during elections, the government should publicly clarify the structure, responsibilities and accountabilities of the bodies involved in its crisis response.

Establishing the basis for an elections information crisis response protocol through the Elections Bill – rather than simply announcing a protocol as a policy – would serve an important legitimating function. By including provisions for a protocol in the Bill, the Government would open up the policy to receive much-needed Parliamentary scrutiny and debate in a way which is vital for building public trust. Moreover, placing the protocol on a legislative footing would ensure that its significance for the operation of elections is accurately reflected in its constitutional status affording more independence from government and crucial protections in the event of any future democratic backsliding. The terms of the provision in the Bill should be flexible enough to allow for the Government to draw up a detailed protocol in consultation with civil society.

For comparison, the [European Union's Digital Services Act](#) 2023 (DSA) includes a crisis response mechanism intended to address the risk that content circulating on digital platforms may amplify a crisis situation⁶. The mechanism allows for the EU Commission to "identify and apply specific, effective and proportionate measures" which digital services must take "to prevent, eliminate or limit any such contribution" to a crisis situation. While the mechanism does not address elections specifically, these would fall under the scope of its definition of crisis. The DSA's crisis mechanism provides a helpful illustration of how the legal basis for a crisis protocol may be set out without overly specifying the content of such a protocol.

Meanwhile, Canada has a [Critical Election Incident Public Protocol](#) which can be taken as inspiration. This is a public document which sets out:

⁵ Parliamentary question regarding the Canadian-style critical election incident protocol, <https://questions-statements.parliament.uk/written-questions/detail/2025-01-08/HL3892>

⁶ EU DSA (2023), Article 36. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>

- A definition of an election incident.
- The responsible body for declaring election incidents: a panel of senior civil servants.
- The minimum threshold for declaring an incident.
- Key considerations the panel must take into account when making decisions.
- Human rights due diligence requirements for the panel, such as a duty to balance freedom of expression rights with the right to free and fair elections.
- Guidance for the panel in administrating the protocol
- Where the panel is to receive intelligence from
- Reporting and transparency procedures, including requirements for public reporting on the outcome of the panel's work after elections.

Recommendations

The UK government should establish a publicly available and transparent protocol for how the Government will respond to future electoral information incidents. This should detail the official body responsible for implementing the protocol, procedures for identifying and responding to crises, transparency and reporting requirements, and its relationship with existing civil contingencies mechanisms. The protocol should set out clear conditions under which it would be triggered. These mechanisms should allow civil society to flag potential information incidents to the Government to trigger the protocol. The protocol should be developed with consultation from civil society, undergo human rights due diligence, and have Parliamentary oversight.

As part of the protocol, the UK government should provide a definition of information crises during elections. This should cover: time limits, severity levels, specificity regarding which people and what systems/platforms are affected, and attribution of what actor(s) have triggered the crisis.

The Elections Bill could set out the legislative basis for such a public protocol. Doing so would allow the protocol to undergo public scrutiny before it is implemented and would grant it Parliamentary legitimacy. The provision in the Bill should include wording to the effect that the Government will establish a protocol to address information crises during election periods. The wording should specify that the Government must develop the protocol in consultation with civil society, that the protocol should be made public, that it should include protections for human rights, and that the Government should report regularly to Parliament on its activities in support of the protocol.