



ELECTHER



THE JO COX  
FOUNDATION



FAWCETT  
SOCIETY

---

## ELECTIONS CODE OF PRACTICE BRIEFING - FEBRUARY 2026

### REPRESENTATION OF THE PEOPLE BILL

Online protections for those taking part in democratic life are long overdue. The Representation of the People Bill is an opportunity to bring in measures to address this through a simple amendment to the Online Safety Act. This briefing note provides an overview of the context, detail on our proposal along with the text of a proposed amendment. Further detail is [available here](#) and representatives of those supporting this briefing are available to provide additional briefing on request.

#### Rationale

Over the past decade a growing body of evidence has shown how online abuse and disinformation, particularly targeting women and minoritised communities, is harming democratic participation and leading to elected representatives choosing to stand down, or prospective candidates deciding not to stand at all.

The [Speaker's Conference](#) and the Public Administration and Constitutional Affairs Committee (PACAC) have both highlighted the role of online platforms in enabling these harms. Following the 2024 General Election, [PACAC explicitly called for Ofcom](#), working with the Electoral Commission, to set out a clear timetable for addressing online abuse and intimidation during elections.

The [Electoral Commission](#) has urged stronger action from both platforms and Ofcom under the Online Safety Act (OSA). In their recent report, following evidence submitted by the Online Safety Act Network, the Speaker's Conference [called for the Government](#) to require Ofcom to produce an Elections Code of Practice to force tech platforms to take action.

*“Noting that elections are high risk periods for abuse and given the significance and authority of codes of practice within the structures of the Online Safety Act, the Government should consider the merits of mandating Ofcom to produce an elections code of practice for social media platforms, and the feasibility of introducing this requirement as part of the Bill it has said it will bring forward during this Parliament on electoral reform.”*

The Government has not yet responded to the Speakers Conference report and - despite the MHCLG [press release](#) claiming the Representation of the People Bill would deliver “much-needed measures to protect candidates, campaigners, and electoral staff from abuse and intimidation, deterring people from taking part in public life” - currently there are no specific provisions in the Bill as introduced that reflect this. Mentions of online abuse, social media and related harms are entirely absent. We urge MPs of all parties - on an issue which has cross-party impact and will have been experienced on an individual level by all - to ensure that this gap is filled.

### Why do we need it?

These harms are not new, but they are persistent and worsening with the rapid development of AI technologies such as deepfakes. Online abuse has become a daily reality for many MPs and candidates, with elections identified as especially high-risk periods.

A new report released by the [Inter-Parliamentary Union \(IPU\)](#) in February 2026 found that 71 per cent of lawmakers surveyed globally experienced violence from the public both online and offline. Furthermore, the [Electoral Commission, who found that](#) 70% of electoral candidates they spoke to had experienced abuse or harassment, including social media abuse, physical abuse, and threatening behaviour during the 2024 UK election. One in five respondents avoided using social media (23%) or putting up campaign materials (20%) as a result of the abuse they faced. Research by Amnesty International found that online abuse was [worse for Black and Asian female MPs](#).

The consequences for democratic participation are profound, silencing diverse voices, disproportionately affecting women and people from minoritised backgrounds and undermining the democratic process.

### What next?

We think that it's essential that tech companies take responsibility for the online safety of candidates and campaigners during election periods, backed by a clear shared understanding of what constitutes electoral harms and unacceptable online behaviour towards them. This includes threats of violence, stalking, online harassment, hate speech, non-consensual deepfakes, doxxing, impersonation, and false statements.

An Online Safety Act code of practice, to be produced by Ofcom in consultation with the Electoral Commission and National Police Chiefs Council, would provide a more consistent approach that protects candidates and gives them the confidence to participate.

This builds on recommendations in the [Electoral Commission's report](#) that "social media and online platforms should do more to help develop improved screening tools for candidates' digital profiles, to remove abusive content and identify perpetrators" and the [Speakers Conference report](#) which said that "the vast majority of abuse and intimidation MPs receive takes place online and social media platforms are a significant source of that abuse for MPs and candidates".

The organisations that endorse this briefing have written such a Code, which aligns with the OSA framework and sets out clear expectations on platforms for protecting electoral candidates online. **We urge the Government to use the Representation of the People Bill to amend the OSA and embed these protections into law to safeguard democratic participation for everyone.**

#### **Insert into Representation of the People Bill, after clause 74**

##### **74A**

(1) Amend the Online Safety Act by inserting into s 41 a new-sub-section (3A) as follows:

(3A) In addition to the Codes required by sub-sections 41(1),(2),(3) and (4), OFCOM must prepare and issue a code of practice for providers of Part 3 services recommended for the purpose of compliance with the relevant duties in relation to electoral harm.

(2) Amend the Online Safety Act by inserting into s 41 and new-sub-section (11) as follows:

(a) Electoral harm means:

(i) illegal content

(ii) content harmful to children and,

(iii) in relation to Category 1 services, content listed in section 16,

directed at candidates, representatives elected as a result of a relevant election, campaign staff, returning officers and associated staff, or their families during an election period.

Electoral harm includes threats of violence, stalking, online harassment, hate speech, non-consensual intimate images including deepfakes, doxxing, offences within the Representation of the People Act 1983, false statements within the meaning of s 179 as well as content or behaviours relating to a foreign interference offence within the National Security Act insofar as each affects a relevant election

(b) Relevant election means all national, local government elections, devolved administration, strategic Mayoral elections and Referenda and national by-elections for and by-elections for devolved administrations.

##### **Notes**

The Online Safety Act envisages that Ofcom will draft a number of codes to help service providers comply with their duties under the Act. This amendment in subsection (1) adds to the codes that Ofcom is required to produce and aims to deal with the specific risks relating to the election period.

To clarify the scope of the amendment, subsection(2)(a) identifies electoral harm, drawing on the existing categories of harmful content covered by the Online Safety, and also

identifies the specific group requiring protection during election periods, which are periods of high risk: candidates (who are defined in the Representation of the People Act 1983), elected officials, campaign staff, election administrators (ie returning officers as defined in the Representation of the People Act) and people working with them on the election, or their families of any of these groups of people.

Subsection(2)(b) delineates the types of election to which the proposed code applies.

## **OSA Network amendment on Election Offences**

Insert into Representation of the People Bill after Clause 74 as Clause 74B

(1) Schedule 7 to the Online Safety Act 2023 (priority offences) is amended in accordance with paragraph (2).

(2) After paragraph 38 insert:

Election Offences

39

(1) An offence under section 66 Representation of the People Act 1983 (requirement of secrecy)

(2) An offence under section 66A Representation of the People Act 1983 (exit polls)

(3) An offence under s 106(1) Representation of the People Act 1983 (false statements of fact as to candidates)

(4) An offence under section 114A Representation of the People Act 1983 (undue influence)

### **Notes**

Some election offences clearly fall within the definition of relevant offences for the purposes of s 59(5) Online Safety Act (eg s 106), though it is uncertain whether all the election offences do (see eg s 66). Yet they are all important for protecting candidates and safeguarding the integrity of elections. Insofar as there are relevant offences, they are, non-designated offences and therefore only subject to base level duties in the Online Safety Act. Moreover, the focus of Ofcom's guidance and enforcement activity has been on priority offences. Listing these offences as priority offences for the purposes of the Online Safety Act will not only confirm that they are relevant offences but give them more visibility, but impose more pre-emptive duties in relation to them.

Note there are 4 separate offences under s 66; it is the intention that all should be listed as priority offences. Section 66 pertains to the secrecy of elections and how people vote; if this information was leaked online (either by the voter or by some other person) this could affect the outcome of the election as it may change how other people vote in response. A similar concern can be found in relation to s66A and exit polls.

Section 106(1) covers making or publishing false statements of fact in relation to the candidates personal character or conduct, unless there are reasonable grounds for

believing, and the person making the statement did believe, the statement to be true and could be triggered by false statements in general but specifically deepfakes.

Undue influence involves threats of various sorts to compel any voter to vote or refrain from voting and could be triggered by content posted online, including misinformation.