Written evidence submitted by Online Safety Act Network to the Representation of the People Public Bill Committee (RPB01)

Summary

1. Online protections for those taking part in democratic life are long overdue. While the Representation of the People (RoP) Bill amends the Elections Act 2022 in relation to hostility to election staff, this is a very limited measure and does not go far enough to address the problems that are now well recognised. The RoP Bill, in its current form, is silent on measures to address online abuse, intimidation and harassment of candidates despite the lived experience of the vast majority of Parliamentarians, their staff and their families. Elections are particularly high-risk periods within our democracy and our society.

2. We ask that the Bill Committee consider amending the RoP Bill to introduce a simple amendment to the Online Safety Act (OSA) for a code of practice which would place responsibilities on services regulated by the OSA to bring in enhanced risk assessments and implement protective measures to protect specific groups of people – including candidates, elected officials, campaign staff, election administrators and their families – from electoral harm.

3. We also recommend that a number of existing offences under Electoral Law are brought more clearly into the scope of the OSA, by including them in Schedule 7 (Priority Offences) of the Act so that the full range of existing illegal content duties apply to them.

4. This submission provides an overview of the context, detail on our proposal to introduce a code of practice (along with a draft of such a code of practice attached as an annex and also available here[1]) and the text of the two proposed amendments to the RoP Bill.

Rationale

5. 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

[1] The code has been developed by the Online Safety Act Network, CCDH, Full Fact, Fawcett Society, Jo Cox Foundation, ISD, Demos, Westminster Foundation for Democracy and Elect Her.

down, or prospective candidates deciding not to stand at all.

6. 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; prior to the 2024 Election, the Joint Committee on the National Security Strategy raised a number of concerns with the then Prime Minister, Rishi Sunak, about risks and threats to democracy, including social media activity and threats to candidates, to which the Home Office responded later in the year.

7. 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."*

8. The Government has not yet responded to the Speaker's 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.

9. 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.

10. 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.

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

Our proposed solution

12. Tech companies must take greater 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 candidates, campaigners and election officials.

13. 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 Speaker's Conference accepted our recommendation for a code of practice to be introduced to address this. **Our draft code (attached at the annex), which was developed in conjunction with experts from CCDH, Full Fact, Fawcett Society, Jo Cox Foundation, ISD, Demos, Westminster Foundation for Democracy and Elect Her, demonstrates how it would work.**

14. In summary, 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. It would bring in enhanced risk assessments and protective measures to protect specific groups of people – including candidates, elected officials, campaign staff, election administrators and their families – from electoral harm.

15. By electoral harm we mean the abuse and intimidation which could discourage the identified groups from freely participating in the democratic process. It would cover

existing categories of harmful content covered by the OSA (illegal content and content harmful to children) as well as the types of harmful content (including abuse based on Protected Characteristics) set out in the Act's user empowerment duties. So, for example, some of the relevant content would therefore include: threats of violence, stalking, online harassment, hate speech, NCII (incl. deepfakes), doxxing, existing ROPA offences, false statements (s 179), content relating to Foreign Interference offence.

16. Our proposal is that this code and the related duties would apply during the defined "regulated period" of elections. We acknowledge that elected national and local representatives, and their staff and families, face high levels of online abuse and threats all year round – and that situation is getting worse. However, to ensure that these important protections can be delivered and we do not inadvertently open up diversionary arguments about the OSA and its reach, we have limited the scope to align with the scope of the RoP Bill.

17. We provide the text of a proposed amendment below.

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.

Bringing election offences into the OSA framework

18. Our second proposed amendment brings existing election offences, which are important for protecting candidates and safeguarding the integrity of elections, into the Priority Offences schedule in the OSA, meaning that stronger duties for companies will apply to them and they will be more within the purview of Ofcom's enforcement activity (which has to date been focused on Priority Offences listed in schedules 5, 6 and 7 of the OSA, rather than on the "non-designated offences"). Bringing them into the Priority Offences schedule means that the OSA's existing illegal content duties would apply to them, including mitigating the risk of those offences occurring on platforms and having a system in place to swiftly remove content related to those offences and minimise the time it is present. It is a straightforward "tidying up" amendment, comparable to other recent amendments the Government has brought in to bring other illegal offences, such as self-harm or NCII, into the OSA.[2]

19. We provide the text of the proposed amendment and the offences we propose to include below.

[2] See here: https://www.gov.uk/government/news/online-safety-laws-to-strengthen-to-protect-people-of-all-ages-from-devastating-self-harm-content and here https://www.gov.uk/government/news/crackdown-on-intimate-image-abuse-as-government-strengthens-online-safety-laws

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; it 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.

March 2026