ONLINE SAFETY ACT NETWORK

DELIVERING IMPROVED ONLINE SAFETY FOR CANDIDATES DURING ELECTIONS: A PROPOSAL FOR A CODE OF PRACTICE

Professor Lorna Woods OBE & Maeve Walsh

Introduction

Online protections for participants in the democratic process are long overdue, with numerous studies over the last decade indicating problems from abuse, particularly directed at women and others with protected characteristics. The previous Government had an opportunity to include measures in the Online Safety Act, but failed to do so. The Speaker's Conference is currently undertaking a deep dive into the security of candidates, MPs and elections and will be publishing a second report shortly on the impact of social media. As part of its work, the Conference has flagged the need to tackle disinformation as a driver of abuse, and recommended a code of conduct for campaigning. The Government's planned code of conduct is intended to address misleading campaigns.

Our proposal would sit alongside that code, for consideration in the context of the Government's recently published Election Strategy, ahead of an Elections Bill anticipated in the next session. It also aligns with the existing codes of practice which are enforced by Ofcom under the Online Safety Act; we note that their new proposal for the addition of a crisis response protocol to the illegal harms codes is currently out for consultation. The crisis response protocol – given it anticipates *ex post* responses - covers different ground from the proposals here.

As the Online Safety Act has demonstrated, it takes time to legislate and even longer to get the subsequent regulatory frameworks in place and enforceable. There is no time to lose if the Government is serious about developing concrete proposals which can be implemented swiftly and embedded before the run-in to the 2029 General Election is upon us. This policy brief sets out such a proposal. It builds on an initial recommendation the authors made, in conjunction with William Perrin, in work for Carnegie UK in 2021 and supplements the high-level framework set out in the Online Safety Act Network submission to the Speaker's Conference earlier this year.

Our proposal

Our proposal is for **the introduction of a duty on Ofcom to produce a code of practice, in consultation with the Electoral Commission and National Police Chiefs' Council and others, to address the potential**

harms arising during the electoral process. An amendment to the Online Safety Act to deliver this duty should be added to the forthcoming Elections Bill and we provide the suggested wording for that below.

We also set out below a potential structure for the code of practice to demonstrate how it would work. The framework follows that used in our earlier work to develop codes of practice to reduce specific online harms. These include: a code to reduce online violence against women and girls, which we co-produced with experts in the sector and which influenced the previous Government to introduce a requirement into the OSA for Ofcom to produce VAWG guidance; a code on hate speech and ad hoc advice on hate speech for the UN Special Rapporteur; and a model code which demonstrates how this approach can align with different regulatory frameworks in different jurisdictions.

We will work with civil society and academic experts in the coming months to develop a full draft of the code on electoral harms and will publish that in due course. Do please get in touch with us if you would like to talk to us about this work, or contribute to its development: hello@onlinesafetyact.net

Commentary

The Speakers' Conference has shone a light on the role that online platforms play in the proliferation of harms to the democratic process. The recent PACAC report on the 2024 general election also highlighted this, recommending "that Ofcom in coordination with the Electoral Commission set out the timescale for setting up arrangements to address online abuse and intimidation at elections."

These harms are ever-present, nor are they new as the research we reference below demonstrates. The appalling levels of online abuse faced by elected representatives on a daily basis has become a fact of life for MPs. Ofcom has recently published research on the impact of such abuse on women in politics. As far back as 2017, the Committee on Standards in Public Life noted in its report on Intimidation in Public Life that:

> '*Some MPs and candidates have disengaged entirely from social media due to the intimidation they have received; others who may be interested in engaging in public life are being put off by the tone and intensity of political discussion online.' (page 31)*

The report also noted that elections are particularly high-risk periods.

> *'By their very nature, elections are competitive and adversarial, and political tensions run high during election campaigns. Social media provides a means by which citizens can engage with the political process during these times, but the darker side of such engagement is the intimidation that Parliamentary candidates, party campaigners, and others in public life experience.'*

The impact of this leads to a potential silencing of voices: research from the Inter-Parliamentary Union in 2016 noted the particular impact on women, the UK Government in 2018 also looked at the issue and a Commons Library briefing from 2021 details the Parliamentary debates on the topic up until that point. Amnesty International published an influential report in 2018 on the levels of abuse experienced by women on Twitter; and the Fawcett Society included a section on abuse in its 2023 report on Modernising Parliament.

The abuse also leads to individuals deciding to leave political life, and democratic participation, entirely. Recent analysis by the Local Government Chronicle found that 52% of local councillors cited online abuse as a factor in their decision not to stand for election; a number of high-profile female MPs who chose to stand down in 2019 cited online abuse as a factor, as also reported by the BBC. Their exit damages the marketplace of ideas by skewing it towards dominant and entrenched views and it seems to have a particular gendered aspect. Those in minoritised groups are likely also to be badly affected; intersectional groups likely most of all.

The freedom of speech implications of this are significant. In our previous work, we have noted that, within jurisprudence related to freedom of speech, the Court of Human Rights has noted that "*while freedom of expression is important for everybody, it is especially so for an elected representative of the people. He represents his electorate, draws attention to their preoccupations and defends their interests*" (*Castells v Spain*, para 42). Further, the Court has repeatedly held that genuine and effective exercise of freedom of expression does not depend merely on the State's duty not to interfere, but may require positive measures of protection even in the sphere of relations between individuals (see eg Dink v Turkey, para 137).

There has been no action to address this. And the Electoral Commission's report on the 2024 General and Local Elections highlighted that the problem is getting worse with female candidates more likely to experience abuse, threats and harassment online than men.

The Commission called for social media and online platforms to "do more to help develop improved screening tools for candidates' digital profiles, to remove abusive content and identify perpetrators" It also called on Ofcom, to "consider how the new duties and responsibilities introduced by the Online Safety Act could be developed in the future to improve online protections for candidates and campaigners".

Despite some awareness during the passage of the Online Safety Bill that the intimidation and harassment of candidates and campaigners was on the rise - and the Puttnam report's recommendation that the "duty of care" should be extended to actions that undermine democracy - the then Government chose not to include any protections for them through specific duties on regulated services or on the regulator itself. It is time to rectify this and the Elections Bill is the obvious opportunity.

Legal context

International human rights law gives considerable scope for Parliament to make rules about speech to protect the electoral process and/or people from harm. The United Kingdom has a strict approach to political advertising on broadcast media (see discussion of the issues in the Neill Committee report) and the Advertising Standards Authority has recently called for regulation of non-broadcast political advertising. The Chief Executive of the ASA called for political advertising to be regulated in 2020 and suggested that: "Experts from several appropriate regulators could take on the task." The Committee on

Democracy and Digital Technologies echoed this in its 2020 report, recommending that experts from the ASA, Electoral Commission, Ofcom and the UK Statistics Authority “should co-operate through a regulatory committee on political advertising” and that parties should work with them to develop a code of practice “that restricts fundamentally inaccurate advertising during a parliamentary or mayoral election, or referendum.”

As a point of comparison, the European Commission has issued guidance for elections under the Digital Services Act, which has some content obligations with regard to promoting official sources of information, as well as more systemic requirements and a specific reference to AI-generated content. The guidance has been used as a basis for monitoring platform responses and actions in the context of several national and EU-level elections over the past year or so. The EU Code also includes foreign interference campaigns; while there is plenty of additional work required by the Government to address election integrity and foreign interference, this is not the focus of our proposed amendments and this code. In addition, a Political Advertising Regulation has also been introduced in Europe.

Proposed legislative changes

The Government should require Ofcom to lead on addressing harms arising from the operation of online platforms during the electoral period, with a requirement on them to consult with the Electoral Commission and the National Police Chiefs’ Council to produce an elections code of practice. In addition to amending the Online Safety Act to deliver this shared obligation, the Government should ensure that the Electoral Commission has the powers and resources to contribute to this work. The code of practice on online electoral harms should also be informed through consultation by the regulators with victims of harm, political parties and platforms amongst others.

We propose the following amendment to the OSA to bring this requirement into force:

> Insert new subsection - s 41(3A):
> OFCOM must prepare and issue a code of practice describing measures recommended for the purpose of compliance with the relevant duties so far as relating to content and activity likely to lead to electoral harms.
>
> Insert in s41(6) after (j)
> (ja) in matters relating to electoral harms, the Electoral Commission and the NPCC
>
> Insert new subsection – s 41(10A)
> In this section “electoral harms” mean content and activity, including abuse and harassment of or threats directed towards elected representatives, candidates, party campaigners and election officials, or incitement to violence against any such individuals, which are likely to have actual or foreseeable adverse effects on an electoral process in the UK. “Electoral harms” does not include mockery or insult, save where it forms part of a campaign of harassment.

Notes on amendment:

Note that "relevant duties" is a defined term – and includes the user empowerment tools when those are in force.

The new definition of "electoral harms" aims to outline the area under consideration and to ensure that legitimate criticisms are not caught by the code.

The phrase "content and activity" comes from the wording for the VAWG guidance.

"Actual or foreseeable effects" comes from the DSA. (See Full Fact's Elections Bill briefing on the case for alignment.) There is language from the UK but it seems narrower (and relates to election offences) - "threats which impede or prejudice the integrity and probity of the electoral process" (Crown Prosecution Service guidance on prosecuting election offences, reviewed and updated October 2019).

The obligation is limited to UK elections but would seem to cover both national and sub-national elections: including Mayoral elections, Welsh Assembly elections, and referendums.

Implementation

The final code should be consulted upon and be a public document. To assist with the thinking required for this process - and to expedite something that is urgently required - we propose that the code should cover at least the points raised below. We will work further on this framework to produce a full draft code in the coming months.

The application of the code should be proportionate to risk of harm agreed with the regulators. By default the largest elections and referendums will be high risk. However, some small elections such as by-elections for Parliament or local authorities might still carry a high risk of harm.

We also propose that Ofcom (and by extension the Electoral Commission and NPCC) should report to Parliament after each major set of elections on the effectiveness of harm mitigation carried out under this regime.

An amendment to bring that into effect for Ofcom via the OSA is provided here:

Insert at OSA S157a

> Ofcom must produce and publish a report assessing-
>
> (a) how providers of regulated services have implemented the measures set out in the Elections Code or taken other appropriate measures
>
> (b) how effective those measures have been
>
> (c) whether there are factors that have prevented or hindered the effective implementation of measures under the Elections Code.

Towards a code of practice

Following on from our proposal to the Speaker's Conference, we set out below how the main components of an electoral harm code of practice should be delivered within the structure we have previously suggested in our work on VAWG and hate crime. We provide in the Annex a skeleton for this code, which we will work on further with experts and stakeholders in the coming months.

The main components and mitigation steps in the regulators' code of practice should include:

- A thorough risk assessment process, including a risk owner with experience of prior UK elections and a requirement to publish a forward look of their plans for all elections in the year. A risk assessment is already required by OSA in relation to illegal content harms and where relevant content harmful to children (and Ofcom has provided guidance). These do not however look at the issues from the perspective of elections and the risk to candidates, MPs and relevant officials. This point should be picked up in the code.

- A helpline service for candidates and MPs that actually works, with standards of performance set out by the regulator in consultation with candidates.

- Appropriately trained case workers assigned to groups of candidates or MPS by the platforms to help them manage problems.

- Established routes of communication and escalation between platforms and Parliamentary online security team.

- Tools for candidates and MPs that help them manage risk according to their tolerance. For instance – filters that protect against certain things. Again this builds on suggestions already made by Ofcom in its illegal harms code

- Features to increase friction, for example rate modifiers to dial down the rate at which messages can be sent (a feature Facebook offers in its groups and that WhatsApp uses in crises).

- Introduction of prebunking measures.

- Adjustment of terms of service to protect participants in the democratic process more effectively and in particular to make clear that abusive and threatening material is not content that is intended to contribute to political debate.

- Terms of service changes to increase penalties for threatening candidates and MPs and tougher action on repeat offenders who breach terms of service – this could take a range of forms including deprioritisation, demonetisation and banning of an account (or duplicate/throw away accounts).

- Platforms interfacing with national and local police in a more effective manner. One mechanism might be to view these institutions as trusted flaggers – along with moderators and fact checkers more generally - and prioritise communications from them in connection with election related threats.

Councillors and election workers should receive the same protections. We set out the detail of each component below.

For the code to function effectively, we propose that the regulators in consultation with regulated platforms and democratic actors will determine performance levels and KPIs for each significant platform.

Transparency and audit

Significant platforms should be more transparent during electoral periods, in particular of the activity of those charged with implementing the code. Daily data should be published on their platform's activities in respect of elections, the nature of that data to be agreed with the regulator. Published data should include information about complaints made and their path to resolution.

The proposals we put forward above codify and enhance best practice to allow democratic actors to make best use of significant online platforms and should address many harmful issues which arise from the operation of online platforms.

ANNEX: The skeleton code of practice

[Note: *We will work with civil society and academic experts in the coming months to develop a full draft of the code on electoral harms and will publish that in due course. Do please get in touch with us if you would like to talk to us about this work, or contribute to its development*: hello@onlinesafetyact.net]

Section 1: Company orientation towards reduction of harm

Our previous codes have included a number of principles within this section, including: Responsibility, Risk Assessment, Mitigation and Remediation; Safety by Design; Education and Training; and Supply Chain Issues.

The starting point in our model code was that the company had to accept responsibility. Risk assessment is particularly key here. Large platforms already plan for risks around major elections and some have nominated contacts for major political parties for instance on political advertising. We suggest formalising and building upon this.

We might suggest that services take the following measures in the code:

a. Appoint a senior, public-facing Elections Risk Manager working in the UK, with experience of prior UK elections to own risks arising from the operation of the platform during electoral periods and the mitigation of that risk (a Senior Risk Owner: Elections ("SRO: Elections"));

b. Assess election-specific risks arising from the operation of their platforms on a rolling basis and publish that assessment.

c. Within this assessment, the risks to likely candidates and other participants should be determined and managed by

> i. Surveying a representative sample of those people for their perception of risks, with particular focus on minority and minoritized groups
>
> ii. publishing a forward look of their plans for all elections in the year (like the BBC annual election guidelines) and
>
> iii. consulting the NPCC electoral violence specialists, senior officers of political parties, the EC and Devolved Authorities.

d. Consult publicly on the risk assessment including OFCOM, NPCC, the EC, political parties and DAs to ensure that the correct risks are covered.

e. put in place a mitigation plan for the risks of harm agreed with all actors and regulators that reflect the risk profile of types of actor;

f. After each major election publish a lessons learned report

Section 2: Access to platform and creation of content

Under this section, we propose working up measures relating to two key principles - in line with our previous draft codes: access to the service; and creation of content.

The Online Safety Act already requires that regulated platforms will have to reduce harm arising from harassment and intimidation of platform users and others. The existing code of practice on illegal harms is therefore a core component of protections for participants in the elections process even before any electoral measures are put in place. The electoral-specific code will supplement the existing duties in that regard.

However, as democratic actors are a defined high-risk group, regulated platforms should take extra steps to reduce the risk of harm to democratic actors from harassment and intimidation. For some the risk will be continuous, for others only around an election period. The measures should be rooted in victim experience and overseen by the regulators. This will require regulated platforms to play a more active, responsive role than has been the case previously.

Significant platforms are currently open to all and this should be formalised. Official Candidates in elections (who have had their papers accepted) should have fair, reasonable and non-discriminatory access to significant platforms. Candidates will be expected to follow platform rules. The online safety regime should improve the operation of enforcement and appeals processes in general – candidates unhappy with the application of platform rules will have access to the enhanced procedure via the SRO Elections.

Access to the service measures will also include terms of service expectations for users of the service: the code should require platforms to adjust their ToS to make clear - both to candidates and other participants in elections as well as other users - that participants in the democratic process should receive specific protections when using the service. There should also be more robust penalties from providers for users of the service who abuse or threaten candidates and campaigners.

The volume and frequency of online abuse targeted at democratic actors is significant, as we detail in our introductory section above. This mirrors the level of abuse that can be directed at other public figures - such as sports stars, journalists or celebrities - where the cumulative effect is both threatening and distressing. The code of practice might therefore include measures relating to the creation of content, such as rate modifiers to dial down the rate at which messages can be sent (a feature Facebook offers in its groups and that WhatsApp uses in crises).

Section 3: Discovery and navigation

We have made a number of suggestions in our model code work on particular measures relating to the way that discovery and navigation tools can facilitate harm to individuals and would propose that we adapt them here for the electoral context.

Section 4: user response, user tools

This section would include measures relating to three principles: user-empowerment tools; virality; reporting and complaints.

The OSA includes a duty on Category 1 platforms to introduce user-empowerment tools, to allow users to manage the content that they see in their feeds. User empowerment tools are also included in the illegal harms code, though there are limitations on how these are used. This will be a key tool for individual candidates to protect themselves from the worst levels of personal abuse and intimidation, in particular that related to protected characteristics. Ofcom will be consulting on this tool in early 2026 so consideration might be given in that work to how the tool might be modified or scaled up to provide extra protections, where needed, during election periods. The election code of practice might then require platforms to pay particular attention to the effectiveness of this tool during election periods and to add in extra levels of responsiveness if candidates have concerns about its use.

We proposed measures in our model code that would reduce the ease of forwarding, or requiring users to click on posts before you can forward them – as well as things like the impact of likes (and this can be on the content creator and not just the person liking). Services should also develop pre-bunking tools to help users navigate the information environment.

Democratic actors are a recognisable group that suffer increased risk of harm and require rapid solutions to threats of harm that arise online. Accordingly, the SRO: Elections should have sufficient resources to provide an expedited rapid response and dispute resolution service to democratic actors. Such a service will build upon the existing reporting and complaints measures mandated in the online safety act via the illegal harms and protection of children's codes under the OSA. The enhanced service standards offered by the SRO: Elections should be agreed with the regulator and interested parties. The service would address the full range of harms arising in a manner proportionate to risk of harm. The service standards should be informed by the election forward look and increase when risk increases such as around election periods.

Section 5: Platform response

This section would include measures relating to moderation, survivor support and remediation and national law.

We note that Ofcom is currently consulting on additional safety measures for their illegal harms and children's codes of practice, which include proposals for user barring and other sanctions. Depending on the final outcome from these consultations, we propose that the elections code should link to these measures with a further commitment from platforms to tougher action on repeat offenders who breach terms of service in relation to attacks on, or targeting of, participants in the democratic process. This would be particularly important in the period running up to an election campaign and during the election period itself.

Platforms also need to put additional resources into support and remediation for victims of online abuse or harassment, for example by assigning case workers to groups of candidates or campaigners to help them manage problems.

Specific measures also need to be identified that will ensure effective and prompt interfacing between national and local police to address specific targeted or coordinated campaigns against individual candidates, particularly in high-profile seats.

The code might also require category one platforms to operate a helpline service for candidates and campaigners during an election period that actually works, with standards of performance set out by the regulator in consultation with existing and former MPs and candidates. There should also be a requirement on platforms to prioritise and triage any interactions and complaints from high-risk, high-profile participants (particularly former MPs or those standing in seats which are of particular national interest or likely to be highly contested) during the election period and to put in place a real-time monitoring system to identify emerging risks, trends or patterns of behaviour across the reports they receive.

Online Safety Act Network

September 2025