



**The Speaker's
Conference**

Speaker's Conference

Second Report

Speaker's Conference on the security of MPs,
candidates and elections

Speaker's Conference (2024)

On 14 October 2024, the House passed a Motion to establish a Speaker's Conference as follows:

That this House considers that it is essential that elections to the United Kingdom Parliament are conducted freely and fairly, without threats or violence; that candidates are able to campaign in safety, with appropriate protection and support; and that elected representatives can do their job securely, and accordingly agrees that the following Order be made.

That:

(1) There shall be a committee to be known as the Speaker's Conference which shall consist of the Speaker, who shall be Chair, and up to 14 other Members appointed by the Speaker.

(2) The Conference shall consider the factors influencing the threat levels against candidates and MPs and the effectiveness of the response to such threats, and make recommendations about the arrangements necessary to secure free and fair elections and the appropriate protection of candidates at future UK-wide parliamentary elections and of elected representatives thereafter.

(3) The Speaker shall appoint one or more of the members of the Conference to act as vice-Chair in his absence.

(4) Except as provided in this Order, the Conference and any sub-committee thereof that the Speaker shall appoint shall conduct its proceedings in such manner as the Speaker shall determine, notwithstanding any Standing Order or practice of this House.

(5) The Conference shall have power—

(a) to send for persons, papers and records, to sit notwithstanding any adjournment of the House and to adjourn from place to place;

(b) to report from time to time;

(c) to appoint legal advisers, and to appoint specialist advisers either to supply information which is not readily available or to elucidate matters of complexity within the committee's order of reference.

(6) The Speaker shall have power to appoint sub-committees of the Speaker's Conference and sub-committees appointed under this order shall have power to send for persons, papers and records, to sit notwithstanding any adjournment of the House, to adjourn from place to place, to report from time to time their formal minutes, and shall have a quorum of three.

(7) The quorum of the Conference shall be five.

(8) This Order shall have effect until the end of the current Parliament.

Current membership

[Sir Lindsay Hoyle](#) (Speaker; Chorley) (Chair)

[Lee Anderson](#) (Reform UK; Ashfield)

[Mr Clive Betts](#) (Labour; Sheffield South East)

[Kirsty Blackman](#) (Scottish National Party; Aberdeen North)

[Samantha Dixon](#) (Labour; Chester North and Neston)

[Zöe Franklin](#) (Liberal Democrat; Guildford)

[Dr Rupa Huq](#) (Labour; Ealing Central and Acton)

[Leigh Ingham](#) (Labour; Stafford)

[Jessica Morden](#) (Labour; Newport East)

[Ben Obese-Jecty](#) (Conservative; Huntingdon)

[Rebecca Paul](#) (Conservative; Reigate)

[John Slinger](#) (Labour; Rugby)

[Sir Mark Tami](#) (Labour; Alyn and Deeside)

[Sammy Wilson](#) (Democratic Unionist Party; East Antrim)

[Sir Jeremy Wright](#) (Conservative; Kenilworth and Southam)

Publication

This Report, together with formal minutes relating to the report, was Ordered by the House of Commons, on 15 October 2025, to be printed. It was published on 27 October 2025 by authority of the House of Commons.
© Parliamentary Copyright House of Commons 2025.

This publication may be reproduced under the terms of the Open Parliament Licence, which is published at www.parliament.uk/copyright.

Conference reports are published on the Committee's website at <https://committees.parliament.uk/committee/741/Speaker-s-Conference-2024/> and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Speaker's Conference (2024), House of Commons, London SW1A 0AA. The telephone number for general enquiries is 0207 219 5944; the Committee's email address is Speakersconference2024@parliament.uk.

Contents

Summary	1
Introduction	4
1 Public attitudes	6
Public attitudes and education	6
Understanding the nature and drivers of abuse	6
The role of education	10
The role of the press	18
Press coverage driving public attitudes towards politicians	18
Reporting practices and sense of safety	21
2 The Criminal Justice Response	26
Overview	26
Policing	26
A more consistent approach to policing	26
Elections law policing	36
Prosecutions	38
Courts and Sentencing	41
Court processes	41
Sentencing for anti-democratic crimes	45
3 Social Media	51
Introduction	51
The role of social media in UK politics	51
Abuse on social media	54
The role of social media platforms	56
Protections for users	57
Meta's and X's response to abuse	60
Mitigations	61

Broader safety measures	64
The Online Safety Act and social media regulation	71
Strengthening the Online Safety Act 2023	75
4 Conclusion	81
Annex 1: Conclusions and Recommendation from the First Report of the Speaker’s Conference on the security of MPs, candidates and elections (HC 570)	83
Annex 2: Speaker’s Conference submission to the Editors’ Code of Practise Committee	92
Annex 3: Draft statutory aggravating factor (hostility to the democratic process)	95
Conclusions and recommendations	97
Appendix 1: 23rd Meeting of the Speakers of The Lower Houses of the G7 Declaration	115
Formal minutes	119
Witnesses	121
Published written evidence	124
List of Reports from the Committee during the current Parliament	127

Summary

We are fortunate in the UK to live in a vibrant democracy. Those who have had the chance to be candidates or MPs are deeply aware of this, and of the privilege it is to represent constituents. This democratic system relies on robust political discourse during campaigns and in Parliament. However, democracy is weakened by abuse, intimidation and personal attacks, which stifle debate and dissuade candidates from standing. We have felt the most extreme impact of this through the murders of two colleagues, Jo Cox MP and Sir David Amess MP.

As covered in our first report, improvements to existing security measures in Parliament and at elections, such as better protection of home addresses and polling stations, can help to keep MPs, their staff and their families safe. However, we concluded in that report that introducing even more security measures would lead to a fundamental and undesirable change in the way MPs engage with their constituents and carry out their roles. The priority instead must be reducing the level of threat posed to MPs and candidates, which has been the focus of this report.

Public attitudes

The perception that it is acceptable to abuse public figures must end. In recent years perpetrators of abuse have been emboldened by a perception that threats and intimidation in politics are becoming more accepted. This is not helped by social media platforms normalising the idea that MPs and candidates should be expected to endure more abuse than people in other professions by showing greater tolerance for abusive content that targets politicians and other public figures. In reality, the majority of people continue to regard abuse as unacceptable and understand that, if they disagree with a decision by someone in public office, they should hold them to account through appropriate democratic and legal means, not by intimidation. There must be effective citizenship education in schools and targeted at the wider public to counter the perception that it is acceptable to abuse politicians and help people understand how to engage positively with MPs, candidates and the political system. As set out in our first report, the Speaker will work with political parties and the Electoral Commission to develop a campaigning code of conduct so that candidates and MPs can set the example for how to engage effectively and challenge constructively.

Abuse and intimidation of an MP or candidate is often triggered by media coverage about them. A free press is a core pillar of democracy and the media are not responsible for how the public react to stories. However, the press must avoid oversimplification or misrepresentation of stories, which can lead to threats, and end journalistic practices like doorstepping at homes that are themselves intimidating.

The criminal justice response

The criminal justice system must do more to deter anti-democratic offences targeting MPs and candidates. These kinds of crimes are damaging but rare, and as a result the response from local police forces and prosecutors is inconsistent. This weakens the deterrent effect of the criminal justice system. The police and prosecutors handling these cases need to have, or be able to access, greater expertise in the issues involved.

The police and Crown Prosecution Service should both have small specialist teams to investigate and prosecute anti-democratic crimes, including abuse and intimidation of elected officials. The new police unit should be introduced in a phased approach, beginning with the establishment of a National Police Chief's Council portfolio to improve consistency and senior ownership of investigations of crimes targeting MPs and Parliamentary candidates.

The Government's decision to introduce a new statutory aggravating factor for offences targeting candidates, campaigners, elected representatives, or electoral staff is a welcome step: this will send a strong message that crimes like these will not be tolerated. The Government should ensure that it covers crimes that are motivated by hostility towards elected officials but directed at their staff or representatives, who are often on the front line of abuse and intimidation.

Social media

The vast majority of abuse and intimidation takes place online. Social media platforms can be useful ways for MPs and candidates to engage with constituents and voters, but they have no constitutional role and the impression that MPs are required to make themselves available to their constituents on social media platforms is entirely false. What is more, the benefits they bring often come at significant cost. All MPs should protect themselves, their staff and the quality of online debate by using protective tools, such as restricting replies, blocking abusive constituents, and ultimately leaving platforms that pose a greater risk than benefit.

For as long as people continue to use social media as a mouthpiece for abuse, responsibility for tackling this issue lies with the platforms. However, we have no faith that the social media companies we have spoken to will address the underlying factors that drive abuse on their platforms unless they are legally obliged to do so. The Online Safety Act 2023 has the potential to deal with many of these issues, but to do so effectively Ofcom must make full use of the regulatory powers it has been given. It must be given time to implement the Act fully, but when appropriate, success of the Act as it relates to the issues under our consideration must be measured by the lived experience of politicians online. Notwithstanding the Online Safety Act's potential, the centrality of social media and constant progress of technology make it highly likely that further social media regulation will be needed at some point, and the Government should be preparing for this now.

Next steps

This is the final report of the Speaker's Conference. We await a response from the Government and other bodies to whom we have made recommendations, and will review and publish these responses in line with normal committee practice. We remain grateful to everyone who submitted evidence, completed the survey or shared their experience by other means, especially when this involved recounting details of distressing events, and to all those who continue to work to protect MPs and candidates.

Our inquiry has highlighted the severity, in volume and nature, of threats to MPs and candidates, and the damage it is doing to democracy. We stand firmly by the view that this is not part of the job and encourage everyone to engage positively in the political process, with courtesy and respect in discussions, and grace and understanding towards those with whom they disagree. Despite the chilling evidence we have received, we are confident that current trends can be reversed and hope that the recommendations of our two reports help shape an agenda for change.

Introduction

1. On 14 October 2024 the House of Commons passed a Motion establishing a Speaker's Conference. That Motion directed the Conference to investigate threats against parliamentary candidates and MPs, and the effectiveness of the response to those threats. We were also directed to make recommendations about the appropriate protection of candidates and MPs, and about securing free and fair elections.¹
2. The Conference divided its inquiry into two phases of work. Our report published on 2 June 2025 marked the conclusion of the first phase. That report focused on understanding the scale and nature of threats against candidates, MPs and elections, and the effectiveness of the response to them. It laid the foundations for our second phase of work and defined the areas of focus for this report, as set out below. The consolidated list of conclusions and recommendations from that report can be found at Annex 1.
3. Our first report identified a significant change in the nature and level of abuse experienced by politicians, with 96% of MPs responding to our survey reporting that they had experienced at least one form of abuse, intimidation or harassment. Such incidents reduce MPs' sense of safety and cause distress and anxiety, not only for themselves, but for their staff and family. Even more concerning, we concluded that the level of threats against MPs and candidates is stifling debate and weakening democracy. It is dissuading people from standing for election and improperly influencing the political choices of those in office, as they are forced to weigh the public good against their own safety and the wellbeing of their colleagues, their staff and their families. These findings highlighted the need to understand better the public attitudes that drive this behaviour. As part of that work, we undertook to explore how social media and the press shape people's attitudes and behaviours towards politicians.
4. The Conference's assessment of the effectiveness of the response to these incidents focused on the police and Parliamentary Security Department (PSD).
5. Our overarching conclusion in relation to the police was that the response to incidents of abuse or intimidation against politicians is inconsistent, within and across forces. This issue is not unique to the police but stretches across

1 Votes and Proceedings, [14 October 2024](#)

the criminal justice system. Whilst we heard some examples of excellent engagement and case handling, inconsistency in the police response, prosecutorial decisions and judicial outcomes weakens the deterrent effect and empowers perpetrators. We therefore undertook to carry out an end-to-end review of the criminal justice response to crimes that undermine democracy and identify recommendations for how it could be strengthened.

6. In respect of PSD's response, the Conference found that whilst there has been a significant step change in the security measures provided by PSD, many MPs still feel unsafe in their role. However, we concluded that a further step change in vulnerability reduction measures would lead to a fundamental and undesirable change in the way MPs carry out their roles and engage with their constituents. Our survey findings also highlighted that MPs' sense of safety is being significantly undermined by online abuse, against which physical security measures have limited impact. We therefore concluded that when it comes to increasing MPs' sense of safety, the focus must be on threat reduction. Understanding what is driving the threat level and the ways it can be reduced is at the heart of this report.
7. Chapter One considers the public attitudes that lead people to consider it acceptable to engage with politicians in an aggressive and abusive way. It considers the role of print and broadcast media in influencing people's perceptions of politicians and political institutions. Chapter Two addresses the criminal justice response, from policing to prosecution and sentencing. Finally, Chapter Three explores the role of social media in driving the level of threats against MPs and candidates.

1 Public attitudes

Public attitudes and education

8. Our first report concluded that “increasingly people think it is acceptable to engage with politicians in a confrontational, aggressive manner. ... We will consider the public attitudes that drive this behaviour, and the ways such societal tendencies can be halted and reversed in our second phase of work.”²

Understanding the nature and drivers of abuse

9. As we outlined in our first report, almost all MPs (96% of those responding to the survey we conducted) had experienced at least one instance of harassment, abuse or intimidation. For most, this is “low-level” abuse that nonetheless has a corrosive effect on MPs’ and candidates’ ability to do their jobs.³ However, a small number of individuals receive an extremely high volume of abuse, many times higher than other MPs and candidates, often spiking around particular events or periods when they are more in the public eye.⁴
10. It is not clear why perpetrators choose to abuse MPs and candidates: the Parliamentary Security Department (PSD) told us that “For the majority of security incidents, the motivation of the perpetrator cannot be immediately determined.”⁵ They are more likely to target some MPs and candidates based on their personal characteristics. Dr Sofia Collignon, Senior Lecturer in Comparative Politics, Queen Mary University of London, told us that “if you are a member of an under-represented minority, an ethnic minority, or a woman—because the perpetrator will always try to use what is unique or special about you as a person—you are an easy target. They take your identity and make abusive comments based on that.”⁶ As a result,

2 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 18

3 [Q136](#) [Oliver Davis]

4 [Q80](#) [Professor Margetts]; Florence King (PhD Researcher at Swansea University) ([SCS0015](#)); Reset.Tech ([SCS0004](#))

5 Parliamentary Security Department ([SCS0045](#))

6 [Q79](#); This was confirmed by Dr Diana Maynard (Senior Research Fellow at University of Sheffield); Professor Kalina Bontcheva (Professor at University of Sheffield) ([SCS0014](#))

the Electoral Commission found that at the last general election, female candidates were twice as likely to be threatened, and ethnic minority candidates were three times as likely.⁷

11. Although the motivations of individual perpetrators are difficult to identify, the behavioural trend is partly driven by shifting societal attitudes and the perception that abusing public figures is more acceptable.⁸ This affects not only MPs and candidates but journalists,⁹ judges,¹⁰ sportspeople¹¹ and other public figures. This phenomenon is not unique to the UK, but a global trend.¹² The international scope of harassment and abuse targeting legislators was highlighted in the Declaration of the 23rd Meeting of the Speakers of the Lower Houses of the G7 (the full document can be found at Appendix 1).
12. Our evidence highlighted three potential reasons for this phenomenon in general and as it relates specifically to politicians: lack of trust in public institutions, poor understanding of politicians' roles, and online behaviours transferring to offline interactions.
13. Several witnesses argued that the increase in aggressive and abusive treatment of public figures is driven by an erosion of trust in public institutions because of the perception that they have failed to meet the challenges people face or are concerned about.¹³ We heard that specific incidents, such as the 2009 MPs' expenses scandal, have cost trust.¹⁴ But this sentiment is also a reaction to the inevitable trade-offs and imperfect solutions to the significant and complex challenges facing countries around the world. Professor Karthik Ramanna, Professor of Business and Public Policy, Blavatnik School of Government, University of Oxford, argued that the global rise in abusive behaviour is associated with fear of massive contemporary social and technological changes. He explained that part of the process of addressing such fear is to ensure a proper understanding of the complexity and cross-cutting nature of these issues.¹⁵

7 [Q45](#) [Vijay Rangarajan]

8 [Q199](#) [Elisabeth Costa]; Prof Helen Fenwick, Professor of Human Rights, Durham Law School, agreed that "The line has moved in terms of people's perception of what is acceptable" ([Q201](#))

9 Dame Sara Khan DBE ([SCS0039](#))

10 The Law Society Gazette, "[Judges have received death threats, LCJ reveals](#)", 26 February 2025

11 Ofcom, "[Sports stars suffer impact of online abuse in real world](#)", 16 May 2025

12 [Q202](#) [Professor Karthik Ramanna]

13 [Q77](#) [Dr Sofia Collignon]; [Q199](#) [Liz Moorse]; [Q202](#) [Prof Karthik Ramanna]; The Jo Cox Foundation ([SCS0008](#))

14 [Q171](#) [Anushka Asthana]

15 [Qq 202, 209](#)

14. Witnesses told us that the rise in threats specifically against MPs and candidates is also partly due to a lack of political literacy, particularly about the role and responsibilities of MPs and other elected officials.¹⁶ The Jo Cox Foundation noted that a lack political literacy can lead to misunderstandings around specific policy debates and decisions turning into incidents of abuse.¹⁷ Professor Alan Renwick, Professor of Democratic Politics, University College London, highlighted that the political literacy “knowledge gap” that needs to be filled includes not only technical knowledge of the democratic and political process but also “openness to the idea that someone with a different view is not necessarily malign or dishonest.”¹⁸
15. People may often not be aware that their comments will be received as abuse. Research by Professor Patrícia Rossini, Professor of Political Communication, University of Glasgow, has indicated that much of what is perceived as “toxic” on social media is people using rude or uncivil language to disagree on a political issue, and is separate to deliberately intolerant, abusive or threatening content. She recommended that intolerance should be distinguished from rude disagreement, and that the latter was not necessarily threatening nor inherently incompatible with online discourse.¹⁹ However, it remains extremely unpleasant for MPs, candidates or anyone to receive, especially regularly or in volume. It is also often ineffective at changing the mind of the recipient or the wider public: behaviour by campaigners that is seen as abusive “will not help them win. ... It is not just that it is not nice to behave like that; the public do not want to see it.”²⁰
16. We review how abuse occurs on social media and recommend potential solutions in Chapter Three, but we note here that the rise in social media use has “catalysed” these social factors driving abuse.²¹ Evidence suggested that this is because online disinhibition (the phenomenon of people feeling less accountable for their actions and less empathy for others) means there is more abuse online, and that, as people spend more time on online

16 Professor Susan Banducci (University of Birmingham) et al. ([SCS0030](#))

17 The Jo Cox Foundation ([SCS0008](#))

18 Professor Alan Renwick (Professor of Democratic Politics and Deputy Director of the Constitution Unit at University College London) ([SCS0031](#))

19 Patrícia Rossini, “[Beyond incivility: understanding patterns of uncivil and intolerant discourse in online political talk](#)”, *Communication Research*, 49(3), 26 May 2020, pp. 399–425.

20 [Q34](#) [Elfrede Brambley-Crawshaw]; Jeremy Corbyn MP similarly agreed that “the public are totally put off by negative campaigning” ([Q20](#))

21 [Q202](#) [Prof Karthik Ramanna]; [Q199](#) [Liz Moorese] Our first report also noted “There was a consensus view among our witnesses that the involvement of social media was not coincidental, and the level of abuse is in part driven by the design and decisions of social media platforms.” (Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 19)

platforms, they are becoming increasingly habituated to more aggressive and abusive exchanges and are carrying this behaviour through to interactions offline.²²

17. However, despite the perception that abuse has become more acceptable, it is important to stress that this shift is not widespread, and it is still a minority of people who condone the abuse of public figures. Elisabeth Costa, Chief of Innovation and Partnerships, Behavioural Insights Team, emphasised that “it is still a real minority of people who are perpetrating this kind of abuse”.²³ In one study, showing people examples of violent threats on social media made most people less supportive of online threats, although a small core (14%) continued to believe threats of violence were an acceptable part of politics.²⁴

18. **CONCLUSION**

Most people continue to regard threats against MPs and candidates as unacceptable, and only a small minority of people resort to them. However, this minority is sufficient to lead to most MPs and candidates receiving a persistent stream of corrosive, low-level abuse, along with occasional, highly intimidating spikes in abuse when public attention negatively targets particular MPs and candidates. Like all bullies, the perpetrators often focus on people’s personal characteristics, especially anything that is distinctive about them, meaning that women and people from ethnic minority backgrounds generally receive more abuse.

19. **CONCLUSION**

It is not clear why this small group choose to abuse politicians and other public figures in this way. But in recent years they have been emboldened by a perception that the behaviour is becoming more acceptable and a widespread erosion of trust in political institutions that is partly a reaction to real failings, but partly the result of a lack of understanding about the political process and the complexity of political decision making, which has let people assume that any political disagreements are due to bad faith motives on the other side. We are also concerned that this group do not appear to be deterred from this behaviour by the existing regulatory and legal framework, and appear to believe they can abuse politicians and public figures with impunity. We return to the effectiveness of the criminal justice system in deterring abuse in Chapter Two.

22 [Qq199–201](#) [Elisabeth Costa; Prof Helen Fenwick]; [Q317](#) [Prof Patrícia Rossini]

23 [Q211](#)

24 Dr. Sarah Shair-Rosenfield (Professor at University of York); Dr. Graeme Davies (Professor at University of York); Dr. Robert Johns (Professor at University of Southampton); Dr. Reed Wood (Professor at University of Essex) ([SCS0026](#))

20. CONCLUSION

We are aware that there are active debates about freedom of speech and political discourse. These debates are focused on how people can express their views about political questions. These debates do not relate to our work, which is about how people directly treat individual MPs and candidates. Some of the comments MPs and candidates receive may be legitimate disagreements expressed in a rude or uncivil tone, either due to heightened emotion or a lack of awareness of how they will be received. We are deeply aware of the impact that the decisions politicians make have on people's lives and wellbeing, and understand that people may often feel upset or troubled about a political outcome, or frustrated or dissatisfied with the political system. However, this never justifies deliberate abuse and threats against individual candidates or MPs. Even if an uncivil or abusive comment is not intended to intimidate, it can still undermine the willingness of the recipient and affected bystanders on all sides to engage in the political process, as well as the argument it is meant to support. We therefore continue to urge everyone to engage positively in the political process, to maintain a courteous and respectful tone in discussions, and to extend grace and understanding to those with whom they disagree.

The role of education

- 21.** Several witnesses suggested that one way to address low trust in public institutions and lack of understanding of elected officials' roles and powers is to improve political literacy through education, both in schools and through public awareness campaigns.²⁵

Citizenship education in schools

- 22.** Improving political literacy and citizenship education for young people was identified as a priority. Our first report noted the warnings from the Electoral Commission that, compared to other age groups, a much greater percentage of 18–24 year olds said verbal abuse of politicians was acceptable, and that “if younger cohorts maintain these attitudes as they age, the problem of abuse of candidates can become worse.”²⁶ The

25 The Jo Cox Foundation ([SCS0008](#)); Electoral Commission ([SCS0020](#)); Dr Sofia Collignon (Senior Lecturer in Comparative Politics at Queen Mary University of London), Dr Wolfgang Rüdiger (Reader in Politics at University of Strathclyde), Professor Susan Banducci (Professor in Political Science at University of Birmingham) ([SCS0023](#)); Professor Susan Banducci (University of Birmingham) et al. ([SCS0030](#)); Professor Alan Renwick (Professor of Democratic Politics and Deputy Director of the Constitution Unit at University College London) ([SCS0031](#))

26 Electoral Commission ([SCS0020](#)); [Q45](#); Oral evidence taken by the Public Administration and Constitutional Affairs Committee on 7 January 2025, [Q25](#) [Vijay Rangarajan]

Government has indicated that it will legislate to reduce the voting age for general elections to 16.²⁷ The Electoral Commission and Association for Citizenship Teaching both said that changes to the citizenship curriculum should be implemented alongside any such change.²⁸

23. We have received helpful and concrete proposals on how to structure an effective programme of citizenship education. Specifically, that it should bring together both an understanding of political concepts and a grasp of political competencies to give students the confidence and motivation to actively participate in the democratic process.²⁹
24. Liz Moorse, Chief Executive, Association for Citizenship Teaching, stressed that building knowledge and understanding of relevant concepts, including democracy, human rights, the rule of law,³⁰ and media and information literacy,³¹ is necessary to ensure that students are “speaking from a place of knowledge and understanding” when they engage with issues that concern them. She warned “If we start with just opinions without building up knowledge and understanding, we will have a problem.”³²
25. In line with evidence highlighted above that abuse is driven by a lack of understanding about the complexities of political decision making, the competencies students need to develop should include critical and analytical thinking skills.³³ Citizenship education should give students practical experience of deliberating, discussing, and using the concepts they have been taught in complex, real-world scenarios to define the problem and identify which elements of it can be addressed.³⁴ In particular, this should include learning about the trade-offs involved in policy formation.³⁵ To achieve this there should be opportunities for students to be engaged in decision making in their school communities,³⁶ including potentially having students who are regarded as trusted messengers by their peers shape elements of the citizenship education programme.³⁷

27 DEP2025-0503 ([Restoring trust in our democracy: Our strategy for modern and secure elections](#)) paras 10-19

28 Liz Moorse ([Q211](#)); Electoral Commission ([SCS0049](#))

29 Liz Moorse ([Q207](#)); Electoral Commission ([SCS0049](#))

30 Liz Moorse ([Q207](#))

31 Liz Moorse ([Q207](#)); Electoral Commission ([SCS0049](#)); Prof Helen Fenwick ([Q210](#)); BCS, The Chartered Institute for IT ([SCS0025](#))

32 [Q207](#)

33 Liz Moorse ([Q207](#)); Prof Karthik Ramanna ([Q205](#)); Electoral Commission ([SCS0049](#))

34 Liz Moorse, Association for Citizenship Teaching ([Q207](#)). Prof Karthik Ramanna, Oxford University, stressed the situations students deal with should be much more like “the complexity and mess of real-world situations” than the “neat and well-defined problems” normally used in individual subjects ([Q209](#)).

35 [Q208](#)

36 Liz Moorse ([Q203](#))

37 Elisabeth Costa ([Q206](#)). This would draw on an approach taken in some effective anti-bullying programmes.

26. Liz Moorse told us that teaching through real deliberative practices is complicated and requires trained teachers, as well as clear guidance for teachers on impartiality.³⁸ The Electoral Commission agreed that teachers would need training and classroom resources to facilitate deliberative practices, as well as support and guidance on evaluating their programmes.³⁹
27. Witnesses also said that to properly prioritise citizenship education in the curriculum it should be taught from KS1⁴⁰ to post-16⁴¹ as a discrete programme of study,⁴² and not confused or conflated with PSHE or RSHE⁴³ by schools or national educational organisations.⁴⁴ The Association for Citizenship Teaching also told us that the curriculum does not give sufficient weight to citizenship education, noting that the current framework only has 14 teaching requirements (items that must be taught to students) for secondary school citizenship education, compared to 420 for maths. They said this was “completely out of proportion with the need.”⁴⁵
28. In order to ensure that this evidence could be considered as part of the Department for Education’s ongoing curriculum review, we wrote to the Secretary of State on 24 June to share a summary of our findings.⁴⁶ We were encouraged by the Secretary of State’s response that the Review panel were considering citizenship education at both primary and secondary level as part of their work.⁴⁷
29. **CONCLUSION**
Strengthening citizenship education must form part of any strategy to tackle abuse, harassment and intimidation of politicians. This should begin with a comprehensive programme of citizenship education delivered by trained teachers.

38 [Q207](#); The Jo Cox Foundation ([SCS0008](#)) also highlighted the importance of impartiality and need for teachers to be adequately trained.

39 Electoral Commission ([SCS0049](#)); The Association for Citizenship Teaching said that this should include guidance on how to assess students to demonstrate impact (Association for Citizenship Teaching (ACT) ([SCS0050](#)))

40 Key Stage 1 (KS1) is the first stage of primary education in England, covering children aged 5 to 7 years old, typically in Years 1 and 2.

41 Electoral Commission ([SCS0049](#)); Association for Citizenship Teaching ([SCS0050](#)); Liz Moorse ([Q207](#))

42 Electoral Commission ([SCS0049](#))

43 Personal, Social, Health and Economic education and Relationships, Sex and Health Education, respectively.

44 Association for Citizenship Teaching ([SCS0050](#))

45 Liz Moorse ([Q207](#))

46 Letter from the Chair to the Secretary of State for Education regarding citizenship education, [24 June 2025](#)

47 Letter from the Secretary of State for Education to the Chair regarding citizenship education, [15 July 2025](#)

30.

RECOMMENDATION

The Department for Education's Curriculum and Assessment Review should ensure that the National Curriculum includes a comprehensive programme of citizenship education from KS1 to post-16. Citizenship education needs to start in earnest in primary schools, so that healthy attitudes towards democratic structures and processes are embedded early on. This programme should develop:

- a. knowledge and understanding of key concepts such as democracy, human rights, the rule of law, media and information literacy, and the different roles and powers of MPs, local councillors, and other elected representatives;
- b. competencies, particularly in critical and analytical thinking, which are often emphasised in respect of the needs of the economy, but rarely in respect of the needs of democracy, as well as confidence and motivation to actively participate in the democratic process;
- c. practical experience of deliberating, debating, and applying concepts in real-world scenarios to learn the trade-offs involved in policy formation;
- d. an awareness of how the tone of discussions, particularly uncivil or rude language, affects others participating in or observing the debate, and how abuse and intimidating behaviour towards politicians affects democracy, along with an understanding that abusive behaviour comes from only a small minority of people;
- e. an understanding of the responsibilities citizens have to maintain a healthy democracy, including around voting and participating in the democratic process.

Teachers must receive appropriate training to deliver citizenship education confidently and impartially, and it must be implemented as an integral part of any proposals to lower the voting age to 16.

We invite the devolved Administrations to consider what, if any, changes can be made to citizenship education in the Welsh, Scottish and Northern Irish curricula to ensure they also deliver the knowledge, skills and understanding outlined above.

31. Politicians also have an important role in play.⁴⁸ The Electoral Commission said more direct engagement between students and elected officials would “help young people understand what the role involves, help humanise

48 Liz Moorse ([Q207](#))

politicians and candidates, and increase trust in democratic institutions”. They warned that currently engagement between students and politicians “is quite patchy.”⁴⁹

- 32.** On average, each constituency has 45 schools and they already play a significant role in many MPs’ constituency work. Education is also an important part of Parliament’s work, delivered through its Education and Engagement Team in the dedicated Education Centre building: nearly 69,000 children visited Parliament on a school trip in the 2024/25 financial year, and 2.4 million people participated in UK Parliament Week 2024, an annual educational event run by Parliament to explain how Parliament works and how people can get involved.

- 33. RECOMMENDATION**
MPs should actively engage with young people in their local areas to support citizenship education. To help them to do this effectively, Parliament’s Education and Engagement Team should expand its offer to MPs to include resources for presentations and practical workshops that are designed by educators with expertise in working with different age-ranges. Parliament’s Education and Engagement Team should also extend the training and guidance on working with children that is currently offered to Members of the House of Lords to any MPs who want to take part. The House of Commons should make available the resources to cover this expansion, based on an assessment of anticipated uptake among MPs.

- 34. RECOMMENDATION**
We encourage MPs to engage with students in their constituency. UK Parliament Week presents a good opportunity for them to visit schools. The Education and Engagement Team should help to facilitate these visits, working with MPs and managing the administrative tasks to enable them to meet as many students as possible.

- 35. RECOMMENDATION**
Although the scope of our work covers only MPs and general election candidates, we encourage local councillors and other elected officials to try to engage with schools in their local area in the same way, and for the relevant local government bodies to similarly support them in doing so.

49 Electoral Commission ([SCS0049](#))

Public awareness campaigns

36. Although citizenship education in schools is a crucial part of addressing some of the issues underpinning trends in the abuse of MPs and candidates, it will not reach current perpetrators. For this, Professor Helen Fenwick, Professor of Human Rights, Durham Law School, proposed a public awareness campaign, based on the model of successful awareness-raising public health campaigns (for example those against smoking).⁵⁰
37. Professor Fenwick proposed that a significant part of this campaign should be delivered on or by social media platforms, with the aim of educating users of the platform about what sort of posts or messages would be considered illegal threats or harassment. She said this would be an opportunity “to try to push the line back, so that social media is not seen as an arena where abuse, especially abuse of MPs, can simply occur and, to some extent, become normalised and acceptable.”⁵¹ Elisabeth Costa raised the concern that abuse is already more normalised online, telling us that “there is this real difference between our perception of what is acceptable online versus offline.”⁵²
38. Elisabeth Costa also noted the potential of behavioural science to inform the approach to tackling abuse, saying “While the evidence base is developing, a range of behavioural interventions show promise and could be adapted and tested in the UK.” In particular, she noted the potential for messaging that makes abuse less normalised, by highlighting that most political discussions are respectful, and providing examples of how to engage passionately but respectfully. She noted the effectiveness of prompts like these on social media sites, along with mechanisms on these sites to encourage people to pause and reflect before sending messages that may be considered abusive.⁵³ We will return to specific measures for addressing abuse on social media in Chapter Three.

39.

CONCLUSION

In-school education has the potential to drive a change in the attitudes and behaviour of future voters, but it does not address the abuse of MPs and candidates today. For that, a wider engagement campaign is needed.

50 [Q205](#)

51 [Q201](#)

52 [Q199](#)

53 Behavioural Insights Team ([SCS0052](#))

40. However, we were warned that a public awareness campaign would be more challenging to deliver effectively than a school-based citizenship education programme.⁵⁴ The main challenge, identified by Professor Ramanna, is that:

The very people you are trying to reach—the people who have perhaps lost faith in the electoral process, in traditional parties, in the media or in institutions like Parliament—are not people who are going to be particularly receptive to any effort on the part of MPs, the traditional media or even social media companies to intermediate in this process, because they just do not trust those institutions. If anything, things that you say to that effect might be used against you, in the sense that it will only feed into their distrust of institutions.

41. Professor Ramanna suggested that an effective campaign would involve building bridges with organisations and individuals that encourage or condone abuse and making them part of any campaign to address abuse. He noted the importance of recognising that there will be genuine policy disagreements and suggested that it would be important to start by humanising MPs and candidates to their opponents to reduce their willingness to abuse them.⁵⁵
42. Nick Price, Director of Legal Services (interim), Crown Prosecution Service, also separately suggested raising public awareness of the seriousness with which the criminal justice system treats the prosecution of anti-democratic crimes. (We cover the detail of how criminal threats against MPs are prosecuted, and what improvements could be made, in Chapter Two.) He told us that courts generally take a more serious view of crimes targeting MPs because of the impact on democracy, but that the deterrent effect of this was limited as many people were not aware.⁵⁶

43. **CONCLUSION**

To reach and change the behaviour of people who are willing to abuse or intimidate MPs and candidates it is essential that any such campaign is based on knowledge of the people involved, their motivations, and the most effective and credible ways to engage with them: whilst the scale and impact of abuse is well-researched and understood, these matters are not. We have tried to answer the questions of why people are abusing politicians and how to change this behaviour. But in the absence of comprehensive research to draw on, the evidence base is insufficient to design a campaign that we could be confident would effectively deliver the change that is needed.

54 [Q205](#) [Prof Helen Fenwick]

55 [Q205](#)

56 [Q236](#)

44.

RECOMMENDATION

We therefore recommend that the Government's Defending Democracy Taskforce commission research to understand the identities and motivations of perpetrators of abuse and intimidation of MPs and candidates (from those engaging in repetitive 'low level' abusive behaviours and communications to those committing criminal offences), and the most effective ways to engage with them and deter them from this behaviour. It should consider the role played by online disinhibition in driving abuse and how to address the disparity in what is considered acceptable behaviour on- and offline, as well as the evidence that exists on the value of working with potential antagonists to spread the message, and the importance of humanising MPs and candidates to people who might abuse them. The findings of this research should inform an engagement strategy that seeks to strengthen understanding of the role of politicians, rebuild trust in political institutions, and highlight the corrosive impact of harassment, abuse and intimidation on democracy. The findings of the research should also be shared with the police to inform offender management strategies.

45.

RECOMMENDATION

Developing a targeted campaign will take time. In the interim, work should begin to end the perception that abuse of public figures is acceptable. The Defending Democracy Taskforce should run a public health-style messaging campaign using the full range of legacy and new media channels, and drawing on up to date behavioural change techniques and research, to counter the perception that it is acceptable to abuse politicians. The campaign should make clear that the majority of people still regard threats against politicians as unacceptable, to raise the social pressure on potential perpetrators, and that criminal threats are likely to receive a more serious response from the criminal justice system. Noting that abuse is often driven by frustration and a lack of political literacy, it should inform people of the methods for engaging with MPs, candidates and the broader political process and help them understand how to use these effectively and positively. This campaign should consider using non-traditional spokespeople who are likely to encourage engagement from the target audience.

The role of the press

Press coverage driving public attitudes towards politicians

46. Our first report concluded that “how the press report on politicians and Parliament shapes public attitudes towards MPs and candidates and can add fuel to the fire, which is at best unhelpful, at worst, causes real harm”. We committed to further examine this issue in our second phase of work.⁵⁷
47. This concern is not new. In 2017, the Committee on Standards in Public Life report into the intimidation of parliamentary candidates also warned that the press might “incite intimidation through delegitimising someone’s engagement in the political process” and that the press “must also be careful they are not unduly or unfairly undermining trust in the political system, especially through portraying stories about disagreements as breaches of ethical standards.”⁵⁸ The Committee’s recommendation that “Press regulation bodies should extend their codes of conduct to prohibit unacceptable language that incites intimidation” was not implemented by IPSO or Impress.⁵⁹
48. IPSO and Impress, which regulate print and digital news, and Ofcom, which regulates broadcast media, all have codes of conduct intended to maintain professional standards and to stamp out unethical reporting. These cover topics such as maintaining accuracy and avoiding harassment by reporters, both of which can affect threats against MPs and candidates. However, Anushka Asthana, Chair, Parliamentary Press Gallery, warned that it was not sufficient to have codes if they are not implemented. She said, “we cannot just hide behind the IPSO code. It has to have teeth.”⁶⁰

57 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 22

58 Committee on Standards in Public Life, [“Intimidation in Public Life”](#), Cm 9543, December 2017

59 Committee on Standards in Public Life, [“Intimidation in Public Life: recommendation tracker with progress rating”](#), 17 December 2020

60 [Q190](#)

49. CONCLUSION

As the Fourth Estate, a free press is a core pillar of democracy. It ensures transparency, holds power to account and encourages informed citizen participation. However, just as MPs and candidates have a responsibility to safeguard democracy through their conduct, so too does the media in its reporting. IPSO, Impress and Ofcom must rigorously enforce their codes of conduct and publishers must ensure all journalists they work with, including freelancers, citizen journalists and others they commission or obtain stories from, are clear on their obligations to adhere to those codes.

50. Abuse and intimidation of an MP or candidate is often triggered by media coverage about them. Several respondents to our survey told us that coverage in the press had triggered threats against them. When we raised this issue with Anushka Asthana and David Hughes, Chair, Parliamentary Lobby, they told us that they considered themselves responsible for informing the public about a story, but not for the public reaction to it. David Hughes said “Our responsibility is to inform the public; we cannot police what is said on social media in response to any of our reporting.”⁶¹

51. Although a news story can trigger threats against a subject, Anushka Asthana argued that it is challenging and unhelpful to try and trace back a causal chain to show it directly led to the abuse. She noted that if press coverage of wrongdoing by a public figure led to them being abused, the coverage and the original action could both be seen as leading to the abuse.⁶²

52. CONCLUSION

There is no question that factual, fair reporting on matters of public interest and robust debate and disagreement in the public eye are vital parts of any healthy democracy. We agree that the media is not responsible for how the public reacts to those stories. But all too often news stories result in abusive and intimidating commentary; no matter what stories there are about someone in the press, it is never appropriate to threaten them personally. When mistakes are made by people in public office they should be held to account through appropriate democratic and legal means, not by intimidation.

53. However, not all reporting on MPs or candidates is completely factual or fair. Dr Sofia Collignon told us that major stories on traditional media that only partially cover an issue, or fail to give the subject a right of reply, can have a significant impact on a candidate’s safety.⁶³

61 [Q176](#)

62 [Q176](#)

63 [Q89](#)

54. Anushka Asthana agreed that it is important for journalists to be fair to contributors and ensure they have a right of reply. She and David Hughes suggested that covering even very toxic issues in long-form could reduce the amount of abuse that follows, as long-form reporting takes the heat out of the issue and gives the subjects time to expand on answers. Anushka Asthana confirmed that audiences do want long-form interviews, noting in particular younger generations' appetite for podcasts and online content. She identified the main challenge as getting time from the relevant politicians, especially senior ministers.⁶⁴

55. **CONCLUSION**

Oversimplification or misrepresentation of a story can serve as a catalyst for abuse and create an unnecessary risk to individuals, for which the press must take responsibility and act to mitigate.

RECOMMENDATION

To address this, we encourage politicians and the press to participate more in long-form interviews and coverage, particularly when considering complex matters.

56. Issues are often oversimplified or misrepresented in headlines. Our witnesses confirmed that it is extremely challenging to condense a complex story into a simple headline that appeals to readers. However, David Hughes also acknowledged that there is an issue with headlines not reflecting the balance found in the full article, saying that "Sometimes I read headlines and think, "That does not really stack up.""⁶⁵

57. Our witnesses told us that under press regulation rules headlines must be accurate, but that the assumption is that it will be read in the context of the article.⁶⁶ However, some research suggests that the majority of people only read headlines, and that these often present a perspective that is caveated, or even contradicted by evidence in the article below.⁶⁷ We are particularly concerned about a tendency to present more negative interpretations of stories in the headlines: there is a commercial incentive for newspapers to highlight negative stories as they have been shown to increase the number of people choosing to read a story or to share it online.⁶⁸

64 [Qq 173, 177](#)

65 [Qq180–182](#)

66 [Qq178–181](#)

67 Full Fact, "[The media must stop using misleading headlines](#)", 28 May 2021

68 Claire E. Robertson et al., "[Negativity drives online news consumption](#)", *Nature Human Behaviour* 7, May 2023, pp 812–822; Harvard T. H. Chan School of Public Health, "[Lessons Learned: A negative headline makes it more likely you'll click](#)", 1 May 2023 (accessed 22 September 2025)

58. We asked Impress and IPSO to confirm how their codes of conduct regulated headlines. IPSO told us that its code required the press to take care not to publish headlines not supported by the text and that it would hold editors to account for misleading, distorted or unsupported headlines. However, they also said that “Publishers finding new ways of presenting information that engages readers in a challenging media environment is something to be celebrated, and IPSO does not seek to interfere with editorial discretion over headlines.”⁶⁹ Impress told us that a headline that was likely to create a false impression in a reader could constitute a significant inaccuracy. They noted specifically that a headline which when taken in isolation presented a claim or allegation as fact, could result in a breach of the Impress code.⁷⁰

59. **CONCLUSION**

In a click-bait, fast-read culture, headlines have a key role to play. However, where headlines are disproportionately negative, read without reference to the full article, or trigger unjustified hostility towards their subjects - be they MPs and candidates or other public figures - that can lead to abuse.

RECOMMENDATION

IPSO should amend its press regulation code to specify that a story’s headline should be accurate, and clearly distinguish between comments, conjectures, allegations and facts, when read on its own, in line with the current Impress code. The IPSO Editors’ Code of Practice Committee’s next review of the Code is expected in 2026: the Conference will submit a formal proposal for this change to this review (see Annex 2 for the text of the submission).

Reporting practices and sense of safety

60. As well as concerns that press coverage may trigger abuse, some of the methods used by the press to investigate stories also directly undermine MPs’ and candidates’ sense of safety.
61. The IPSO Editor’s Code of Practice and Impress Standards Code both require that publishers should ensure journalists do not engage in intimidation or harassment when covering a story.⁷¹ This covers both journalists employed by the newspaper, and freelance journalists contributing to a particular

69 Letter from the Chief Executive Officer, IPSO, to the Chair regarding IPSO regulation, [1 August 2025](#)

70 Letter from the Chief Executive, Impress, to the Chair regarding Impress standards code, [30 July 2025](#)

71 IPSO, [The Editors’ Code of Practice](#), ipso.co.uk (accessed 23 September 2025); Impress, [Standards Code](#), impressorg.com (accessed 23 September 2025)

story (a change that was made after the 2017 inquiry by the Committee on Standards in Public Life identified issues with freelance journalists harassing public figures).⁷² However, both codes contain exemptions to permit this behaviour if there is a public interest in doing so. We were told that press organisations take this public interest test seriously and expect serious sanctions if their actions are not truly in the public interest.⁷³

- 62. However, evidence to our inquiry indicates that some journalists are still using aggressive and invasive techniques to investigate news stories. One respondent to the Conference’s survey reported being doorstepped by national media representatives at home, frightening their partner and child.
- 63. We observed in our first report that for many MPs and candidates intimidatory behaviour that occurs at their home, or affects their family, is particularly threatening. As a result, we have a specific concern about the potentially intimidatory effect of journalists “doorstepping”⁷⁴ MPs and candidates at their homes and approaching their families.
- 64. We asked Anushka Asthana and David Hughes what purpose doorstepping at private residences served. They argued that it is a tactic for the press to use when someone has declined to be interviewed for a clip in another setting, but they were unable to say how often it successfully elicited a useful comment.⁷⁵ David Hughes told us that the main purpose of doorstepping was to show the audience the amount of effort journalists are willing to put in to get an answer:

I would say there is value, in that case, of demonstrating to an audience that we have tried. If we are at their house and they walk by and ignore our questions, then you have them getting in the car and driving off or whatever it is. We can say that we have tried and have even gone to the extent of going to their house to see if they will speak to us, they have not, and provide proof that they have not.⁷⁶

72 Committee on Standards in Public Life ([SCS0012](#)); Committee on Standards in Public Life, “[Intimidation in Public Life: recommendation tracker with progress rating](#)”, 17 December 2020; Letter from the Chief Executive Officer, IPSO, to the Chair regarding IPSO regulation, [1 August 2025](#); Letter from the Chief Executive, Impress, to the Chair regarding Impress standards code, [30 July 2025](#); Letter from the Chief Executive, OFCOM, to the Chair regarding journalistic practices, [1 August 2025](#)

73 Anushka Asthana, David Hughes ([Qq191–193](#))

74 Defined as “an attempt to obtain an interview, or piece to camera, from a contributor without prior arrangement or agreement, typically by confronting them in a public space, such as outside their home, workplace or courthouse.” (BBC, [Door-stepping](#), [bbc.co.uk](#) (accessed 22 July 2025))

75 Anushka Asthana ([Qq187, 194–5](#))

76 [Q197](#)

65. IPSO confirmed that under its code, approaching an individual for comment may sometimes be required for accuracy, but that determining whether a journalist was justified in remaining at a private residence after being asked to leave would depend on the specifics of the case and the public interest.⁷⁷ Ofcom also said that doorstepping is only permitted if an interview has been refused or cannot be requested, and must be justified by the public interest: they told us “[e]xamples of public interest could include revealing or detecting crime, protecting public health or safety, exposing misleading claims made by individuals or organisations or disclosing incompetence that affects the public.”⁷⁸ They did not clarify how footage of a person leaving their house would reveal any of this information to viewers.
66. In contrast, Impress said journalists should approach a subject for comment to ensure accuracy but “there is no requirement to make ‘every’ attempt to get a comment from a subject, particularly not by approaching them at their private residence.” Impress appears to have a much higher bar for journalists to justify remaining at a private residence after being asked to leave, telling us:
- Should a journalist decide to remain outside a private residence after the subject declined to comment and requested the journalist to desist, they would have to demonstrate that they had exceptional grounds to conclude that such a request by the subject was an attempt to evade legitimate journalistic enquiries on a matter of public interest (as defined under the Public Interest section of the Standards Code). The public interest here could relate to the uncovering of information which exposes unethical or illegal practices by a public official for example.⁷⁹
67. Part of the reason audiences may expect journalists to attempt to get answers from politicians, or others who are the subjects of press coverage, at their homes is that doorstepping is a long-standing tradition of reporting. However, Anushka Asthana told us that the practice had changed significantly over the last 30 years. She said, “I remember being in massive packs outside people’s homes in the noughties ... and I can totally see that what was happening at the time was wrong.” The press now agree not to knock on people’s doors, approach their children or broadcast information that can be used to identify where a house is. There are also now efforts at

77 Letter from the Chief Executive Officer, IPSO, to the Chair regarding IPSO regulation, [1 August 2025](#)

78 Letter from the Chief Executive, OFCOM, to the Chair regarding journalistic practices, [1 August 2025](#)

79 Letter from the Chief Executive, Impress, to the Chair regarding Impress standards code, [30 July 2025](#)

coordination between press organisations to ensure there are not multiple cameras at people's homes and to withdraw if it is clear no response is forthcoming.⁸⁰

68. However, it is clear to us from conversations with colleagues, and to the public from the footage they see of politicians when they are approached by the press outside their homes, that doorstepping remains an intimidating and invasive experience.

69. **CONCLUSION**

The press's practice of doorstepping MPs and candidates at their homes intimidates them and their families and undermines their sense of safety. It normally produces nothing except a video or a photograph of the person waving away cameras from their house, which adds no information to justify a public interest defence. If anything, the practice of doorstepping when people decline to comment operates as an implicit threat: "Give us a quote, or we'll come to your house."

70. **CONCLUSION**

The practice of doorstepping has evolved over time, but needs to evolve further. In future, if the press truly believe they need to show proof that they have made appropriate efforts to contact someone, any doorstepping should occur at their known place of work, or in another professional setting where they are expected to be.

71. **RECOMMENDATION**

IPSO, Impress and Ofcom should amend their press regulation codes to make clear that doorstepping at a residential address is a form of harassment for which there is no public interest exemption. Doorstepping MPs or other official figures should only be acceptable around their offices and other professional settings. The Conference will include this proposal in its submission to the IPSO Editors' Code of Practice Committee's next review of the Code (Annex 2). Similar changes should be reflected by Ofcom and Impress in their respective codes when they are next reviewed.

72. The Committee on Standards in Public Life drew our attention to an incident noted in their 2017 report in which a parliamentary candidate's young child was accosted by a freelance journalist, causing distress.⁸¹ Changes were subsequently made to IPSO's and Impress's regulatory codes, but we are

80 [Qq 187, 195](#)

81 Committee on Standards in Public Life ([SCS0012](#))

aware of subsequent incidents in which journalists have approached MPs' young children in an attempt to mislead them into revealing information about their parents.⁸²

73. Anushka Asthana confirmed that the press should not approach a public figure's family as part of covering a story: "As for family members, they are not fair game. They are not politicians; they are not in the public eye."⁸³ However, none of the regulators indicated that they have specific requirements or guidelines governing interactions with the families of public figures (although IPSO and Impress have requirements on harassment, and Ofcom requires broadcasters to avoid unwarranted infringements of privacy).⁸⁴
74. Impress and Ofcom both indicated there are no specific requirements under their code relating to when and how journalists can speak to family members of an MP or candidate.

75. **RECOMMENDATION**
IPSO, Impress and Ofcom should amend their press regulation codes to make clear that children, spouses or other family members should not be used as a way of gaining access to or information on an MP, or any other public figure. There should be no public interest exemption for this conduct. The Conference will include this proposal in its submission to the IPSO Editors' Code of Practice Committee's next review of the Code (Annex 2). Similar changes should be reflected by Ofcom and Impress in their respective codes when they are next reviewed.

82 [Q188](#) [Sir Mark Tami]

83 [Q187](#)

84 Letter from the Chief Executive Officer, IPSO, to the Chair regarding IPSO regulation, [1 August 2025](#); Letter from the Chief Executive, Impress, to the Chair regarding Impress standards code, [30 July 2025](#); Letter from the Chief Executive, OFCOM, to the Chair regarding journalistic practices, [1 August 2025](#)

2 The Criminal Justice Response

Overview

76. The second opportunity we identified to reduce the threat level was to improve how the criminal justice system deters threats against MPs and candidates and supports their sense of safety. Our first report stressed the importance of “a consistent, swift response to reported incidents of abuse and intimidation” to achieve these goals, but identified inconsistencies in the way such incidents are dealt with throughout the criminal justice system. We therefore committed to undertaking “an end-to-end review of the criminal justice response to crimes that undermine democracy”, with the aim of addressing inconsistencies. We concluded that we would explore in particular the merits of: a more centralised policing approach; a specific offence or aggravating factor for these crimes; and reconsidering how threats of violence against MPs are classified by the criminal justice system.⁸⁵
77. This section examines how instances of abuse and intimidation against MPs and candidates are treated when they break the law. It notes the challenges and inconsistencies we have found at each stage of the criminal justice process, from the initial police investigation, through the prosecution and court process, to the sentencing of the perpetrator.

Policing

A more consistent approach to policing

78. The police are the first to respond to incidents of abuse and intimidation against MPs and candidates that may break the law. As we outlined in our first report, these cases are investigated by the local police force, in line

85 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, paras 97 and 79

with other crimes.⁸⁶ There are several centrally managed programmes from the police and the Parliamentary Security Department (PSD) to support and provide an overview of these investigations:

- Parliamentary Liaison and Investigation Team (PLaIT): (established 2016) a team in the Metropolitan Police Service which handles crimes against MPs committed in London, and monitors how crimes against MPs are pursued nationally;⁸⁷
- Op Bridger: (established 2016) a police officer in each force who act as experts on the crimes against MPs and Parliamentary candidates and a point of contact for them;⁸⁸
- Op Ford: (established 2024) a similar programme to Op Bridger, but for other elected officials and candidates;⁸⁹
- Elections Specialist Points of Contact: (established 2008) a police officer in each force specialising in elections crimes such as bribery and electoral fraud;⁹⁰
- Consultative Panel on Parliamentary Security: (established 2015) established by Sir Lindsay Hoyle as Chairman of Ways and Means, the panel is composed of Members and senior officials of the House of Commons and House of Lords who support the Speaker and Lord Speaker's discharge of their security responsibilities and facilitate communication between the security leadership and Members of both Houses.

79. The evidence we have heard has shown that these programmes have had a positive impact.⁹¹ However it also highlighted that investigations into allegations of crimes against MPs and candidates suffer from significant inconsistency in the way different police forces, and individual officers within those forces, deal with them, with many not recognising the seriousness of the incidents and threats involved.⁹² This is a significant problem because an inconsistent response to the policing of abuse and intimidation against MPs

86 [Qq106–107](#) [Detective Inspector Barnard]

87 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 74

88 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 74, para 31 footnote 45

89 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 31 footnote 45

90 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 41

91 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 74

92 Metropolitan Police ([SCS0047](#)); [Qq 97, 100](#) [Commander Messinger]; Home Office ([SCS0042](#)); [Q45](#) [DCI Ives]; Metropolitan Police ([SCS0048](#))

and candidates undermines MPs' sense of safety and belief in the value of reporting issues, affects their ability to carry out their role, and reduces the deterrent effect against perpetrators.⁹³

- 80.** Inconsistency stems partly from the challenges of policing crimes with a political dimension, as police officers are concerned about accusations of political bias if they intervene.⁹⁴ Other Parliamentary Committees have recently also noted the extra-complexity of, and the additional training required for, policing crimes with an anti-democratic element: since our first report was published, the Joint Committee on Human Rights has noted that there is also an inconsistent police response to transnational repression,⁹⁵ particularly between police forces due to a lack of training for police officers. The Joint Committee recommended the formation of a dedicated reporting line staffed by specially trained personnel.⁹⁶
- 81.** We were told that whilst PLaiT and Op Bridger endeavour to drive consistency in the police response to threats against MPs and candidates,⁹⁷ they have limited powers. Witnesses therefore recommended the involvement of senior leaders in policing to help drive a more consistent response. Alison Giles CB, Director, Parliamentary Security Department, told us:

The point I really want to land is that the Met, for all its power, has quite limited power when it comes to commissioning work from different forces across the country. One of the things that would be really useful for this Conference to consider is how we collectively better leverage some of the national bodies, such as the National Police Chiefs' Council, where there is greater leverage around chief constables.⁹⁸

- 82.** Oliver Davis, Deputy Director (Members' Security and Risk), Parliamentary Security Department, suggested a model with stronger and more active central leadership.⁹⁹ Chief Inspector Bryan Duffy, the lead officer for Op

93 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, paras 75–79; Metropolitan Police ([SCS0047](#)) noted the risk that inconsistency would reduce victims' confidence in reporting crimes.

94 [Q57](#) [DCI Ives]; [Q90](#) [Dr Sofia Collignon]

95 Crimes against individuals in the UK directed by foreign states which, like threats against MPs, often include harassment and online disinformation and have a chilling effect on freedom of speech.

96 Joint Committee on Human Rights, Seventh Report of Session 2024–26, [Transnational repression in the UK](#), HC 681 / HL Paper 160, paras 1, 51–52, 62

97 [Q100](#) [Commander Messinger]; Metropolitan Police ([SCS0047](#))

98 [Q135](#)

99 [Q136](#)

Bridger, suggested that anti-democratic crimes could be made a portfolio under the National Police Chiefs' Council (NPCC) in line with the model for other areas, like violence against women and girls.¹⁰⁰

83. The Government has supported proposals for greater specialisation and more involvement and accountability from senior leaders to drive consistency in the response to crimes against MPs and candidates. Shaun Hipgrave, Director Protect and Prepare, Home Office, said “Now we have to work with police chiefs to ensure that the top-down strategic lead and the bottom-up support for MPs are consistent.”¹⁰¹ Dame Diana Johnson MP, then-Minister for Policing and Crime Prevention, Home Office, agreed that specialisation “might be a way forward” to achieve consistency, noting the value of having experienced specialists handling these unusual crimes: “when events may happen only very infrequently, we cannot expect police forces and all officers to fully understand the complexities of some of the issues that they are having to deal with around MPs, councillors or candidates.”¹⁰²
84. The NPCC confirmed that “[s]uitable seniority would facilitate the drive for a more consistent approach to key events”, noting that a central approach under NPCC ownership would allow for wider Ministerial oversight, leverage to bring in stakeholder capability, the opportunity to brigade resources to handle urgent crises, agreement on approaches and operations, and ultimately “greater consistency in identifying crimes and prosecutions, thereby minimising the threat posed by individuals.”¹⁰³
85. Chief Constable Gavin Stephens, Chair, National Police Chiefs' Council, also told us that having a national specialist team would improve the policing of these crimes by developing shared intelligence capability. This would give the police more opportunities to intervene early and prevent crimes targeting elected officials, which would be particularly effective in strengthening the police's ability to address situations where the perpetrator has mental health issues, in line with the “offender management” approach several witnesses recommended prioritising for the policing of threats against MPs and candidates.¹⁰⁴ He suggested that a specialist team, focusing on crimes against elected officials, could develop a common intelligence capability for both Op Bridger, covering MPs and Parliamentary candidates, and Op Ford, covering other elected officials

100 Metropolitan Police ([SCS0048](#))

101 [Q149](#)

102 [Qq242-243](#); Alison Giles CB also warned that most police officers may be hesitant about taking forward cases involving MPs because they would not be familiar with them ([Q136](#))

103 National Police Chiefs' Council (NPCC) ([SCS0051](#))

104 [Q136](#) [Alison Giles CB]; [Q109](#) [Detective Inspector Barnard]; Speaker's Conference, First Report of Session 2024-26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 91

and candidates for those roles. This would be beneficial as the individuals who may be targeted often move between, or hold concurrent local and Parliamentary roles.¹⁰⁵

86. CONCLUSION

Following the concerns identified in our first report that an inconsistent policing response to threats against MPs and candidates reduces their sense of safety and weakens the deterrent effect for perpetrators, it is now clear that a national specialist team approach to anti-democratic crimes, led by a senior body like the National Police Chiefs' Council, would improve the consistency of the police response. The relatively small number of MPs and infrequency of electoral events means that crimes targeting them are too rare for all officers to develop the necessary knowledge and understanding—particularly of the political dimensions and impact such incidents have on democracy—to ensure a consistent and appropriate response. This approach would allow a smaller group of officers to develop expertise to support these investigations.

87. CONCLUSION

A central capability with specialist officers provides other benefits. There are opportunities to improve intelligence and better manage offenders before threats escalate, by combining the policing of threats against MPs and candidates with the policing of threats against other elected officials and candidates. There is also an opportunity to include the specialist policing of other anti-democratic crimes, such as the dedicated hotline for reporting crimes directed by foreign states that has been recommended by the Joint Committee on Human Rights.

Models for establishing a specialist team

- 88.** We asked the NPCC to suggest how a more specialist approach would work in practice. They proposed two options, one focused exclusively on MPs and parliamentary candidates, and another covering both this group and other elected officials and candidates. Both models involve the NPCC taking the lead.¹⁰⁶

¹⁰⁵ [Q212](#); [Q220](#); Chief Inspector Duffy has also noted that Op Bridger and Op Ford face many of the same policing issues and that intelligence is not automatically shared if people move between being MPs and other elected roles. However he noted that it should be possible for Op Bridger and Op Ford to share intelligence through their back office teams and IT systems (Metropolitan Police ([SCS0048](#))).

¹⁰⁶ Noting the Government's current work on police reform, the NPCC advised that in future the capability would likely migrate to the planned National Centre of Policing (National Police Chiefs' Council (NPCC) ([SCS0051](#))).

89. The NPCC said that if the desired approach is to give “greater profile and oversight of only Op Bridger”, a viable model would be to create an NPCC portfolio for crimes against MPs and Parliamentary candidates. They told us that this could build on PLaIT’s current set up (based in the Metropolitan Police’s Parliamentary and Diplomatic Protection team and funded by Parliament) but with changes to lines of command and hierarchy. (The NPCC did note that there is already an ambition to expand the Op Bridger and PLaIT infrastructure based on the increase in demand since the general election).¹⁰⁷ Whilst this configuration would expand the capability for orchestrating a more consistent response to anti-democratic crimes targeting MPs and Parliamentary candidates, it would not provide the same intelligence sharing benefits that would come from a model that also covers Op Ford and wider anti-democratic activity. However, this narrower model would mitigate concerns expressed by Detective Inspector Barnard, PLaIT Operational Lead, that merging Op Bridger and Op Ford “could significantly impact the effectiveness of the Op Bridger policing response” given the current lack of clarity on the scope of protection for other elected officials.¹⁰⁸
90. The second model they proposed was a central function covering Op Bridger, Op Ford and other anti-democratic crimes. This could be based on “a familiar concept” of NPCC ownership and direction, such as the model used for the National Police Coordination Centre (NPoCC), which provides intelligence support focussed on assessing strategic threats from protest and monitors national capacity and capability across related specialist skills. They suggested a unit with an NPCC portfolio lead at Chief Officer level and headed by a Superintendent. Its day-to-day work would be to “bring different Force capability and governance consistently in line with current and future national guidance and minimum standards, improving national reporting measures and [to] act as an internal inspection agent.” Noting the Government’s current work on police reform, the NPCC advised that in future the capability would likely migrate to the planned National Centre of Policing.¹⁰⁹
91. Under both models individual crimes would continue to be investigated locally with support and guidance from the central unit. When we asked Chief Constable Stephens how any more centralised approach might work in the context of individual investigations, he suggested that its focus would be on “preventive opportunities” such as removing disruptive online content

107 National Police Chiefs’ Council (NPCC) ([SCS0051](#))

108 Metropolitan Police ([SCS0048](#))

109 The NPoCC provides support to all forces and a central co-ordination function for UK policing. It is made up of a small number of officers and staff drawn on secondment from police forces across the UK and funded by contributions from all forces. Of particular relevance to this topic, it provides intelligence support focussed on assessing strategic threats from protest. (NPCC, [National Police Coordination Centre \(NPoCC\)](#), [mpcc.police.uk](#) (accessed 23 September 2025))

more quickly.¹¹⁰ Sarah Sackman KC MP, Minister of State, Ministry of Justice, supported this approach of having local forces continuing to investigate individual offences supported by a central unit to ensure a consistent approach. She cited work from the Antisemitism Policy Trust that showed that threats against elected officials often involve issues around community relations which benefit from local knowledge from local police forces.¹¹¹

92. Chief Constable Stephens emphasised that any national specialist team should have strong digital capabilities, noting that more than 50% of crime is committed online and that 80% has a digital footprint. He said this should include a focus on opportunities for prevention, such as getting illegal online material taken down quickly.¹¹²
93. The NPCC and Dame Diana Johnson MP agreed that a new specialised unit would require additional resources, although the NPCC noted that even if no changes were made “the current Op Bridger infrastructure for PLaiT and the governance team is looking to expand based on the increase in demand since the general election”.¹¹³ The NPCC noted that the cost of combining Op Bridger and Op Ford would depend significantly on the level of demand from other elected officials: “If the Op Ford cohort was to deliver demand at the same rate [as Op Bridger], a substantial team would be required to successfully deliver against assessment, prevention, investigation and nominal management, even if some elements of this business were left in the hands of local forces. A phased approach would be required to deliver this either at scale or at pace.”¹¹⁴

Alternative models

94. Coordination under the NPCC is not the only possible model for policing particular issues. Some crimes in the UK are investigated as dedicated funded subjects under the National Crime Agency (NCA), who “provide a range of specialist and niche capabilities that are best delivered nationally on behalf of all UK law enforcement.” They note that this is particularly true of major crimes that most police forces will conduct relatively few investigations into and where “it is more appropriate, and cost-effective, for the NCA to retain niche, specialist skills on a permanent basis and be the single point of contact for all law enforcement.”¹¹⁵ Chief Inspector Duffy

110 [Q238](#)

111 [Q255](#)

112 [Q220](#); [Q238](#)

113 National Police Chiefs’ Council (NPCC) ([SCS0051](#)); [Q242](#) [Dame Diana Johnson MP]

114 National Police Chiefs’ Council (NPCC) ([SCS0051](#))

115 National Crime Agency, [Providing specialist capabilities for law enforcement](#), nationalcrimeagency.gov.uk (accessed 14 October 2025)

noted this model as a possibility, but told us that policing should first look to improve consistency and standards across local forces by making anti-democratic crime a portfolio under the NPCC.¹¹⁶

95. CONCLUSION

The models suggested by the National Police Chiefs Council are both potential ways to improve the senior oversight and consistency of policing crimes targeting MPs and candidates, but do not go far enough. Even with more central coordination it will still be challenging for local forces to develop the understanding of the democratic and political issues involved when these crimes are relatively uncommon. Ultimately to deliver this, a dedicated unit for investigating anti-democratic crimes will be required.

96. RECOMMENDATION

To drive consistency, the Government should work with policing to begin a phased process towards establishing a centralised, senior-led unit to investigate anti-democratic crimes, which would include abuse and intimidation of MPs and candidates as well as abuse of other elected officials and related issues like transnational repression. This approach would ensure that policing had the expert capability required to tackle these unusual crimes that it is not cost-effective for local forces to develop. The responsibilities for the protection of MPs and candidates, as well as sites and events of democratic importance, such as homes and offices and campaign meetings, would remain with the relevant local police forces. Responsibility for public order and protests would also not change. The new model should have clear mechanisms to determine what does and does not constitute an anti-democratic crime (in particular ensuring that crimes where the perpetrator did not know or consider that the victim was an MP are not wrongly considered anti-democratic) and the ability to join up local knowledge and specialist expertise. This should include knowledge of differences in legislation between the nations of the UK. It should also have an emphasis on intelligence and digital capabilities and a focus on nominal management and other preventative opportunities.

116 Metropolitan Police ([SCS0048](#))

97.

RECOMMENDATION

The new unit should be introduced in a phased approach, beginning with the NPCC establishing a portfolio under the model of existing programmes like the National Police Coordination Centre to provide intelligence support, coordinate the national response, and develop and monitor adherence to clear national guidance and minimum standards for anti-democratic crimes. Initial stages should build on the existing efforts of PLaIT and Op Bridger to improve consistency and focus on ensuring senior ownership of threats against MPs and Parliamentary candidates, bringing forces in line with advice and guidance and delivering intelligence. Op Ford, which performs a similar function for other elected officials, should subsequently be included in the same programme: integrating Op Bridger and Op Ford should improve the intelligence capability but the currently unknown demand from Op Ford is likely to be a significant driver of cost. The capability should be appropriately resourced at all stages: in particular there must be sufficient understanding of Op Ford's resource needs as well as additional funding and staffing before any integration occurs to ensure that coordination does not result in existing Op Bridger resources being diverted to Op Ford. Once established, the unit should take responsibility for investigating crimes that target politicians because of their roles, and other anti-democratic crimes.

Guidance for local forces

98. The work of a specialist policing function in improving consistency would cover areas in the policing of anti-democratic crimes where reforms are currently ongoing or where we recommended improvements in our first report. National guidance would build on, and ensure the consistent implementation of, the new Defending Democracy Policing Protocol. The Protocol provided refreshed guidance on policing democratic events, and undertakings on how the police would engage with protests. It includes particular undertakings on protests at elected representatives' offices, reflecting the fact that protests at offices affect the staff who work there.¹¹⁷ The Protocol confirms that protests at offices "should not be allowed to (i) prevent or inhibit the use of the venue, attendance at the event or access to and from it or (ii) cause alarm, harassment or distress to attendees through the use of threatening or abusive words or disorderly behaviour, in keeping with public order laws."¹¹⁸
99. The national specialist team's work in providing guidance would also overlap with the recommendation in our first report that:

117 Members' and Peers' Staff Association (MAPSA) ([SCS0032](#))

118 Home Office, [Defending democracy policing protocol](#), gov.uk, February 2024

The police, Crown Prosecution Service and Government should work together to develop guidance that clarifies the criminal thresholds for communications, electoral and public order offences as they relate to incidents of abuse and intimidation of MPs and candidates, or electoral events. This guidance must form the basis of training for returning officers and police officers.¹¹⁹

100. As well as recommending that criminal thresholds be clarified, our first report also questioned whether the classification of threats of violence against MPs under current policy and guidelines appropriately reflects their seriousness and impact on democracy; we resolved to consider this as part of our second phase of work.¹²⁰

101. Jonathan Hall KC, the Independent Reviewer of Terrorism Legislation, suggested that it would be appropriate for some incidents in which individuals threatened to assault or physically harm MPs to be investigated as an act of terrorism. He provided several hypothetical examples of how threats against MPs on social media aiming to influence the government or intimidate the public or a group, such as supporters of a particular policy or MPs in general, could constitute terrorism under current legislation. Mr Hall told us that any incidents investigated under terrorism powers would benefit from quicker and more effective investigations and higher penalties in the case of convictions. He advised that “any coordinated online or coordinated real life attempt to intimidate MPs with threats of violence should at least be considered for investigation as terrorism, in particular where the threat is or appears to be very immediate, or where a campaign is growing, so that it merits an immediate deterrent response.”¹²¹

102. Mr Hall stressed strongly that deciding whether individual incidents should be investigated as terrorism must be at the discretion of the police. Specifically the decision would be made by the Senior National Coordinator of the Counter Terrorism Policing network. Mr Hall also emphasised that not all cases of violent threats against MPs could or should be treated as terrorism.¹²² The case specific nature of the decision was reinforced by evidence on the unique political and security situation in Northern Ireland, where we were reminded that some elected representatives “still live with an overhanging terrorist threat”.¹²³ The Government agreed that police must

119 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 87

120 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 97

121 Letter from Jonathan Hall KC to the Chair regarding the classification of threats against MPs, [9 July 2025](#)

122 Letter from Jonathan Hall KC to the Chair regarding the classification of threats against MPs, [9 July 2025](#)

123 [Q43](#) [Timothy Johnston]

use their discretion to decide whether an incident meets the definition of terrorism, considering both the circumstances of the case and whether the use of counter-terrorism powers would be “necessary and proportionate”. They stressed that Counter Terrorism Police must determine how to allocate resources to investigations, noting the significant number of live investigations that pose a higher threat to the public. Nevertheless, the Government noted that having a central police body collating local forces’ responses to threats against MPs “allows for assessment and response from that force or escalation to counter-terrorism policing if required”. Currently local forces report on these cases to PLait, but as discussed above we have heard proposals, and made recommendations for how this central team could be strengthened.¹²⁴

103. CONCLUSION

From an early stage, the NPCC’s aim and responsibility should be to ensure that police forces’ investigations into criminal threats against MPs and candidates follow national guidelines, to bring in external stakeholder and coordinated policing resources to deal with crises, and to develop the shared intelligence and preventative measures to stop threats escalating. This should include ensuring forces fully implement the Defending Democracy Policing Protocol’s provisions on ensuring that protests at constituency offices do not impede the use of the venue or threaten or abuse attendees; and taking the lead on developing and disseminating the guidance to clarify criminal thresholds which we recommended in our first report. This guidance should include advice to local forces on when it would be appropriate to consider investigating threats against an MP or candidate as terrorism, what powers and capabilities would be available to do this and how to seek advice from the NPCC lead on when to refer a case to Counter-Terrorism Policing. This advice should acknowledge the unique history and security situation in Northern Ireland. In order to ensure counter-terrorism powers are used appropriately, the NPCC lead should establish a dedicated liaison and good working relationship with the Counter-Terrorism Policing network.

Elections law policing

104. In our first report we noted that the current policy of having dedicated elections single points of contact (SPOCs) separate to the Op Bridger and Op Ford networks may fail to reflect the shift in elections related crimes from offences like bribery and fraud to intimidation. As noted above, the elections SPOCS are their force’s expert in elections crimes, such as fraud and bribery. They also have a responsibility to understand their force’s approach to

124 Letter from the Security Minister to the Chair regarding the harassment and intimidation of MPs, [23 September 2025](#)

harassment and tell candidates and campaigners about relevant material on dealing with threatening behaviour. However, the local force's Op Bridger lead and Force Elected Official Adviser are responsible both during and outside elections for issues related to the security of their respective elected officials and candidates.¹²⁵ We committed to consider whether a different structure for policing anti-democratic crimes could manage this change in elections related crimes better.¹²⁶

- 105.** Commander Simon Messinger, then-Commander, Protection, Metropolitan Police, suggested that there might be an opportunity to combine, or better coordinate, the elections and Op Bridger portfolios. He suggested this could work by having the newly introduced Force Elected Official Advisers (full time employees tasked with liaising with and advising elected representatives and candidates, including MPs, on security issues) also serve as elections SPOCs, but noted it was not clear if they would have the capacity or capability. Similarly, when we asked Chief Constable Stephens about the possibility of combining the elections and Op Bridger portfolios he warned that the workload for elections is already extremely high, with a significant increase in the level of reporting. He indicated that intelligence coordination between the two roles was more important:¹²⁷ we have heard that elections SPOCs and Op Bridger leads already coordinate regularly.¹²⁸

125 College of Policing, [Key roles and planning](#), college.police.uk, 12 April 2024 (Accessed 14 October 2025)

126 Each police force has an officer designated as its elections single point of contact (SPOC): they are primarily trained and focused on managing crimes like bribery and electoral fraud. They are separate to their force's Op Bridger and Op Ford leads, but the two teams do coordinate regularly. (Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, paras 41–43)

127 [Q213](#)

128 [Q47](#) [DCI Ives]

106.

RECOMMENDATION

In line with our previous recommendation, elections law policing should, in future, be brought within the remit of the anti-democratic crimes unit. Until then, current arrangements for ensuring each police force has electoral law expertise are still very necessary. However, candidates are now far more likely to be affected by abuse and intimidation than elections law crimes. The expertise of their named point of contact should reflect this. We therefore recommend that Op Bridger leads and Force Elected Official Advisers (FEOAs) should be candidates' named points of contact. The elections single points of contact (SPOCs) should understand the issue of harassment at elections and how to refer anyone affected by it to the Op Bridger lead or FEOA. The NPCC should ensure that the Op Bridger leads, FEOAs and elections single points of contact are joined up and share knowledge and intelligence, at both local force and national leadership levels.

Prosecutions

107. Following a police investigation, a decision is made about whether or not a case should be prosecuted. The Crown Prosecution Service (CPS) explained how this decision is made in England and Wales:

The police and the CPS make the charging decision based on the two-stage test set out in the Code for Crown Prosecutors. The first stage is to ask if there is sufficient evidence for a realistic prospect of conviction: is the evidence such that a court are more likely than not to convict? If the first stage is met, then the second stage is to ask if a prosecution is required in the public interest. If both stages are met, the suspect is charged. The CPS then has responsibility for the conduct of the prosecution thereafter.¹²⁹

The CPS has noted that, although online abuse and harassment of MPs and candidates often fails the evidential test (a point we will return to in Chapter Three on social media), this does not tend to be the case in instances of serious in-person offending. They also note that cases involving elected officials are more likely to pass the public interest test for a prosecution than those involving private individuals.¹³⁰ Where relevant, prosecutors consider a “community impact statement” as part of the public interest

129 Crown Prosecution Service ([SCS0024](#)) In Scotland and Northern Ireland the CPS's role is filled by the Crown Office and Procurator Fiscal Service (COPFS) and the Public Prosecution Service (PPS) respectively.

130 Letter from Director of Public Prosecutions to the Chair regarding the work of the Speaker's Conference, [9 May 2025](#)

test. Such statements illustrate a community's concerns about a crime.¹³¹ In order to support MPs affected by criminal abuse, beginning in 2019 Sir Lindsay Hoyle has provided a regularly updated community impact statement explaining how crimes targeting MPs affect them and the wider Parliamentary community. This statement is considered as part of the public interest test for these crimes.¹³²

108. The CPS itself is divided into 14 regional teams, each headed by a Chief Crown Prosecutor.¹³³ Prosecutors from these local teams generally make charging decisions and prosecute cases for most crimes in their region, including criminal threats against MPs and candidates. Alison Giles CB highlighted that it is difficult to achieve consistent prosecution thresholds within a federated system like this.¹³⁴
109. The CPS has told us that they have some measures in place to try and get consistency through senior and central oversight of cases involving MPs and candidates, “as these cases are considered particularly sensitive given the threat they pose to democracy.” Nick Price, Director of Legal Services (interim), Crown Prosecution Service, also agreed that they are “sensitive and difficult cases, and may not be cases that prosecutors deal with every day.” As a result, Chief Crown Prosecutors must personally sign off cases involving MPs and provide monthly reports on them to the Director of Legal Services, the Director General of Legal Delivery and the Director of Public Prosecutions to ensure that the right charging decisions are made and the cases are being progressed at an appropriate speed. When a case is particularly challenging, particularly if there are complex legal features, it is moved from the regional team to CPS’s central caseworks division where it will be handled by lawyers “who are generally more experienced in dealing with more idiosyncratic cases.” This decision can be made based on set casework acceptance criteria or at the discretion of the Director of Legal Services. Some cases, such as those prosecuted under the Representation of the People Act 1983 (the basis for election offences such as personation, undue influence, and bribery) or those which have a terrorist connection, are automatically prosecuted by central teams.¹³⁵

131 CPS, [Community Impact Statements](https://www.cps.gov.uk/community-impact-statements), cps.gov.uk, 29 October 2019 (accessed 23 September 2025)

132 The first statement was provided before becoming Speaker in his capacity as Chair of the Consultative Panel on Parliamentary Security.

133 CPS, [The CPS Areas, CPSD, CPS Central Casework Divisions and CPS Proceeds of Crime](https://www.cps.gov.uk/cps-areas-cpsd-cps-central-casework-divisions-and-cps-proceeds-of-crime), cps.gov.uk (accessed 23 September 2025)

134 [Q137](#)

135 [Qq214–215](#) [Nick Price]; [Q255](#) [Lucy Rigby KC MP]; Letter from Director of Public Prosecutions to the Chair regarding the work of the Speaker’s Conference, [9 May 2025](#)

110. The CPS told us that they believe “oversight provided by the Directors of Legal Services, including review and testing of casework decisions, ensures these cases are suitably gripped as well as delivering a consistent approach.”¹³⁶ Nick Price said there was sufficient centralised oversight to ensure consistent decisions are being made and delivered.¹³⁷ The then-Solicitor General, Lucy Rigby KC MP, supported the CPS’s assessment, saying “My understanding is that we do not have issues within the CPS that go to discrepancies between regions”, but acknowledged that the broad range of offences that could be involved presented a challenge.¹³⁸
111. Although the CPS’s mitigating measures and the Minister’s confidence in them are reassuring, it is hard to tell how effective they are in delivering consistent prosecutions and outcomes because of a lack of data. Despite the monthly reporting of cases involving MPs, the CPS told us that it does not collect structured data on the profession of the victim. Sarah Sackman KC MP, Minister of State, Ministry of Justice, agreed that “we need to find a way of beginning to collect the data, to monitor the effectiveness of what we already have. ... [W]e have to be able to track sentencing outcomes, conviction rates and so on.”¹³⁹

112. **CONCLUSION**

For decisions on whether or not to prosecute criminal threats against MPs and candidates to be consistent the harm they do to democracy must be consistently accounted for as part of the public interest test. Acknowledging that these cases are damaging but rare, the Crown Prosecution Service (CPS) has put in place measures to ensure senior oversight of prosecutions, although most are still handled at the local level.

RECOMMENDATION

However, consistent decision making is a function of expertise, not seniority, and it would be more effective to have a small team of specialists focused on prosecuting anti-democratic crimes and expertise in electoral law to ensure consistent assessments of the public interest in prosecution of such cases.

136 Letter from Director of Public Prosecutions to the Chair regarding the work of the Speaker’s Conference, [9 May 2025](#)

137 [Q214](#)

138 [Q255](#)

139 Crown Prosecution Service ([SCS0024](#)); [Q265](#)

113. CONCLUSION

Prosecutors can inform their assessment of the public interest of prosecuting with the community impact statement for crimes against MPs provided by the Speaker of the House of Commons. However, this statement does not currently cover candidates or MPs' staff. Reflecting the risk that both face from anti-democratic crimes, the Speaker will work with the Director of Public Prosecutions and the police to expand, or produce new statements, that can be considered as part of the public interest test for crimes against candidates or MPs' staff.

114. RECOMMENDATION

The lack of available data makes it hard to assess the effectiveness of the CPS's approach to ensuring consistency in prosecution thresholds. The Government, through the Defending Democracy Taskforce, must begin to collect 'full picture' data on criminal cases targeting elected officials because of their roles. The Ministry of Justice should be represented on the Defending Democracy Taskforce at ministerial level to reflect the need for a full criminal justice system grip on this issue. Building on the current CPS central oversight of cases involving MPs, a system should be established to track cases referred to CPS, and the charging and sentencing outcomes, as well as applications for protective orders (covered below). The data should be used to identify inconsistency in decisions, which can be used to inform CPS guidance, target training and advice, and help determine the appropriate level of central CPS oversight. The data gathered should also be shared with police and the Parliamentary Security Department on an ongoing basis.

Courts and Sentencing

Court processes

Protective orders

- 115.** When any individual is harassed, courts have powers to issue a variety of orders to prevent an alleged or convicted offender from further contacting a victim or undertaking other specified actions. These orders, which we will refer to broadly as "protective orders", include restraining orders in England, Wales and Northern Ireland, stalking protection orders in England and Wales, and interdicts and non-harassment orders in Scotland.
- 116.** Protective orders can be an important way of ensuring the safety of MPs who are victims of stalking or harassment. They are also an important protection for MPs' staff, who are often on the frontline of abuse targeted at

the MP.¹⁴⁰ Courts are empowered but not required to make an appropriate protective order and they must be applied for by one of the parties involved. We have been told that whether a court decided to make an order in an individual case, and what restrictions it imposed, would be dependent on the specific facts of the case and the positions and arguments of the prosecution, victim and defence. This means that courts often change the provisions of a protective order as the case progresses and new arguments and evidence are introduced.¹⁴¹ Lord Colbeck, Judicial Member, Scottish Sentencing Council, told us that based on his experience he would expect courts to consider a protective order in cases involving stalking. He noted that for some crimes, such as domestic violence, there are already specific provisions in the criminal justice process that establish a presumption that a protective order will be granted, but that these provisions have not been introduced for anti-democratic crimes.¹⁴²

117. One issue is that a protective order's purpose of preventing contact can run counter to the general principle that people should be able to engage with their MP. This can lead to situations where, for example, an individual who had harassed their MP in one instance by sending them a letter covered in white powder had a "robust" restraining order placed on them that still allowed them to contact the MP by letter.¹⁴³ The Sentencing Council's guidance on protective orders in England and Wales does not cover what a court should do if the victim of harassment is the perpetrator's MP.¹⁴⁴
118. Where protective orders are issued, they are not always consistently enforced. Concerns have been raised that the police's awareness and enforcement of protective orders is patchy,¹⁴⁵ and victims are not always kept informed about key developments in a case that may affect their sense of safety, such as details of a protective order, or the perpetrator being released from prison.¹⁴⁶ One MP told us that an individual who had

140 Members' and Peers' Staff Association (MAPSA) ([SCS0032](#))

141 [Qq218-219](#) [Lord Colbeck]; [Q224](#) [Chief Constable Stephens]

142 [Qq218-219](#)

143 BBC, "[Man cleared of stalking MP Rebecca Pow given restraining order](#)", 20 May 2021

144 Sentencing Council for England and Wales ([SCS0053](#))

145 "[A duty to protect: Police use of protective measures in cases involving violence against women and girls](#)" His Majesty's Inspectorate of Constabulary and Fire & Rescue Services

146 The Victim Contact Scheme requires the Probation Service to inform victims of specified sexual and/or violent offences about the offender's release. A review of pilot schemes for informing victims of other crimes found that around 40% of victims were not informed within the target time period and details of restraining orders were often not available (Ministry of Justice, [A Process Evaluation of the Victim Notification Scheme](#), 27 March 2025, pp 2, 23). Our first report noted that that one of the most cited reasons for MPs' or their staff's dissatisfaction with the criminal justice response to threats is not being kept informed of actions or outcomes in a case (Speaker's Conference, First Report of Session 2024-26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, para 94, Annex 1: Survey Findings)

a restraining order preventing them from coming near her simply ignored it.¹⁴⁷ The Government and the police are currently trialling new measures to address this, including new methods for the notification of protective orders from courts to the police, and new technology to monitor them.¹⁴⁸ Currently there is a particular challenge preventing people who are barred from contacting their MP by a protective order from accessing the Parliamentary estate, where the MP may be working, as visitors to the estate are not required to give their name or present ID.¹⁴⁹ This is set to change as the Commissions of both Houses have approved the introduction of a visitor information system.

119. CONCLUSION

MPs are entitled to decide who they and their staff will meet or otherwise engage with. In cases of stalking or harassment protective orders play an important role in ensuring the sense of safety of MPs and their staff. It is therefore unsatisfactory to assume they will be imposed without a mechanism to ensure it, especially as courts may well have concerns about preventing an individual from contacting their MP.

120. RECOMMENDATION

The Sentencing Council and devolved equivalents should produce guidance on protective orders in cases where the perpetrator has targeted an MP or their staff. Guidance should include:

- a. The presumption that a protective order should be imposed, in recognition of MPs' vulnerability due to their public prominence and regular engagement with the public, and staff members' vulnerability due to their public facing role and easily identifiable working location.
- b. Where the perpetrator is a constituent of the MP, a mechanism for how they can still avail themselves of a right to be represented in Parliament without causing risk or alarm to the victim, such as passing communications through an intermediary.

¹⁴⁷ Anonymous ([SCS0044](#))

¹⁴⁸ Police Digital Service, [Press release – Police Digital Service and West Yorkshire Police pilot new process to safeguard victims](#), pds.police.uk, 27 March 2024 (accessed 23 September 2025); College of Policing, [Geofencing software to direct specialist resources to monitor preventative orders](#), college.police.uk, 20 May 2024 (accessed 23 September 2025); Letter from the Ministry of Justice to HMICFRS regarding progress on recommendations given in the “A duty to protect” super-complaint report, [26 May 2022](#)

¹⁴⁹ Members' and Peers' Staff Association (MAPSA) ([SCS0032](#))

121. RECOMMENDATION

As technology is developed to assist police with enforcement of domestic violence protection orders, the Government should explore how this can be used to help frontline police officers enforce restraining orders, stalking protection orders and other court orders intended to prevent people harassing MPs. As noted in our first report, MPs and candidates should be kept informed about key developments that may affect their sense of safety, such as a protective order being imposed or removed, or the perpetrator being released from prison.

122. RECOMMENDATION

Parliament should also support efforts to ensure the enforcement of protective orders. The House service should accelerate plans for a visitor information system. Whilst improving visitor experience, this system will provide an important mechanism to check the identity of visitors to the Parliamentary estate to ensure that individuals who are prohibited from approaching their MP by a protective order are not able to use Parliamentary access to do so.

Election periods

- 123.** UK Parliamentary election periods are short and intense, but people who threaten candidates or campaigners are often not prosecuted until some time after the vote.¹⁵⁰ As the Online Safety Act Network warned “action after an election on material that has affected candidate safety during a campaign is of little use.”¹⁵¹
- 124.** We heard that there are existing arrangements to try and resolve cases during election periods. The then-Solicitor General and Nick Price both agreed that cases where the intent was to affect or disrupt elections must be dealt with quickly. During elections the CPS has a dedicated team of lawyers and designated points of contact in the police to provide early advice on investigations. Nick Price told us that the CPS was looking to further improve these processes for future elections.¹⁵² In addition, the CPS can ask the courts to expedite cases that involve MPs or affect Parliamentary candidates during an election, and “[g]iven the specialised handling of these cases, judges would almost certainly consider requests to expedite proceedings if circumstances allow.”¹⁵³

150 Mr Simon Danczuk ([SCS0021](#))

151 Online Safety Act Network ([SCS0001](#))

152 [Qq234–235](#) [Nick Price]; [Qq266–267](#) [Lucy Rigby KC MP, Sarah Sackman KC MP]

153 Letter from Lucy Rigby KC MP, Solicitor General, to the Chair regarding evidence given to the Conference on 2 July 2025, [8 August 2025](#)

125. CONCLUSION

The CPS and the courts have provisions in place for expediting trials in cases that occur during election periods and which may affect or disrupt the outcome. However, these provisions do not appear to be widely used or effective, as many cases are still not resolved until long after the end of the election campaign.

RECOMMENDATION

The Government and the CPS should set new targets for prosecutors and courts such that all cases of intimidation and abuse of candidates that occur during an election period, and have a reasonable chance of successful prosecution, should be dealt with within days in order to minimise the risk of them influencing the vote.

Sentencing for anti-democratic crimes

Aggravating factor for anti-democratic crimes

- 126.** Our first report concluded that the second phase of our work would give “particular consideration to: the merits or otherwise of a) a specific offence against MPs and b) an aggravating factor applicable to sentencing for crimes committed against candidates or MPs because of their role”. Our intention was to address concerns that the way the criminal justice system currently prioritises crimes against MPs and candidates, which can often be considered “low-level” crimes”, does not properly reflect the cumulative effect of these crimes on democracy.¹⁵⁴
- 127.** There are already aggravating factors for offences targeting people working in the public sector or providing a public service, which includes MPs, candidates and election campaigners.¹⁵⁵ This is a statutory aggravating factor (one set by legislation) for cases of assault and threats to kill in England and Wales¹⁵⁶ and a general non-statutory aggravating factor in sentencing guidance for other crimes.¹⁵⁷

154 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, paras 95–97

155 Sentencing Council for England and Wales ([SCS0005](#)); Scottish Sentencing Council ([SCS0022](#))

156 [Police, Crime, Sentencing and Courts Act 2022](#), s 156

157 Sentencing Council for England and Wales ([SCS0005](#)); Scottish Sentencing Council ([SCS0022](#)); Sentencing Council for England and Wales ([SCS0053](#)); [Qq227–229](#) [Nick Price]; Nick Price and Lord Colbeck confirmed that courts do generally consider the anti-democratic implications of crimes targeting MPs and candidates as an aggravating factor when sentencing depending on the specific facts of the case ([Qq229–233](#))

- 128.** Sarah Sackman KC MP made the case for building on this legislation. She argued that sentencing should reflect the fact that “there is a category difference between those who are elected to serve the public and those who perform other public duties” and attacks targeting elected officials are attacks on democracy. Chief Constable Stephens similarly argued that greater legislative protection would not indicate a greater prioritisation of elected officials as individuals, but would reflect the law and the criminal justice system’s “responsibility for the key pillars of the state—democracy, freedom of the press, our judiciary and policing—to make sure that they can operate freely and fairly”.¹⁵⁸
- 129.** Despite the concerns raised in some evidence that the deterrent effect of new offences or aggravating factors is unclear and may be limited,¹⁵⁹ Chief Constable Stephens told us that legislation aimed at specific crimes “can have a declaratory effect ... by sending a very strong message that certain types of behaviour will not be tolerated.”¹⁶⁰ Nick Price also highlighted the deterrent value of drawing public attention to how the courts treat crimes targeting elected officials, as noted in Chapter One.¹⁶¹
- 130.** The Courts Minister noted that an aggravating factor would be more flexible than a specific offence of abusing an MP or candidate: while a new offence would likely be extremely targeted, a statutory aggravating factor at sentencing would ensure the anti-democratic nature of a crime was considered whatever the offence.¹⁶²
- 131.** After we discussed this issue with Ministers, the Government published its elections strategy. This included a commitment to introduce a statutory aggravating factor for offences motivated by hostility towards candidates, campaigners, elected representatives, or electoral staff. They noted that this would “underline the severity of the offence and give greater protection to those involved in upholding and participating in democratic processes.”¹⁶³

158 [Q248](#) [Sarah Sackman KC MP]; [Q226](#) [Chief Constable Stephens]

159 Sentencing Council for England and Wales ([SCS0005](#)); Scottish Sentencing Council ([SCS0022](#))

160 [Q226](#); The Scottish Sentencing Council also noted that a purpose of sentencing can be to express disapproval of the behaviour (Scottish Sentencing Council ([SCS0022](#)))

161 [Q236](#)

162 [Qq249–252](#)

163 DEP2025–0503 ([Restoring trust in our democracy: Our strategy for modern and secure elections](#)) paras 76–77

132. CONCLUSION

Our first report said we would consider the merits or otherwise of a) a specific offence against MPs and b) an aggravating factor applicable to sentencing for crimes committed against candidates or MPs because of their role. It is clear that there is a case for a specific aggravating factor and that this has advantages over a specific offence because it would be better able to take account of the various ways people may try to intimidate a politician.

133. RECOMMENDATION

We therefore welcome the Government's decision to introduce a new statutory aggravating factor for offences motivated by hostility towards candidates, campaigners, elected representatives, or electoral staff. The Government should ensure this can be applied broadly, including covering crimes that are motivated by hostility to elected officials but directed against their staff and representatives, who are often on the front line of abuse and intimidation of MPs. To this end, we recommend the Government bring forward legislative proposals, at the earliest opportunity, that reflect the elements and spirit of the draft legislative provisions we have included at Annex 3. Governments of the devolved nations should take steps to reflect this change in their own legislation.

134. The evidence we have heard has highlighted the prevalence of abuse targeted at women. The Electoral Commission Report found that abuse and intimidation at the 2024 General Election was “in particular directed at women.”¹⁶⁴ Witnesses have confirmed that this misogynistic abuse is putting women off standing for election.¹⁶⁵

135. However, sex is one of the few protected characteristics not covered by hate crime legislation. Similarly, crimes motivated by hostility to the victim's sex are not treated as aggravated, unlike for other protected characteristics.¹⁶⁶ When we asked Dame Diana Johnson MP about the potential for gender based abuse to be treated in the same way as racial or other abuse, she noted that the Law Commission's 2021 report had recommended against adding sex or gender to the protected characteristics for aggravating offences (this was largely because of potential negative consequences on the prosecution of rape and domestic abuse¹⁶⁷). Dame Diana told us that “the Government's position is that we are reflecting on what the Law

164 The Electoral Commission, [Report on the 2024 UK Parliamentary general election and the May 2024 elections](#), p27

165 [Q1](#) [Bob Blackman MP]; [Q30](#) [Mike Dixon]; [Q96](#) [Will Fletcher, Dr Sofia Collignon]; [Q355](#) [Jessica Zucker]

166 CPS, [Hate Crime](#), cps.gov.uk (accessed 23 September 2025); Sentencing Council, [General guideline: overarching principles](#), sentencingcouncil.org.uk (accessed 23 September 2025); [Equality Act 2010](#) s 4

167 Law Commission, [Hate Crime](#), lawcom.gov.uk (accessed 23 September 2025)

Commission has said. I cannot say to you today what our position is on that today; there is work ongoing.”¹⁶⁸ However, we note that similar reviews into how misogyny is treated under the law in Scotland and Northern Ireland reached different conclusions: the Scottish Working Group on Misogyny and Criminal Justice recommended the creation of a new Statutory Misogyny Aggravation and other offences, and the Northern Irish hate crime legislation independent review recommended that sex/gender should be included as a protected characteristic in hate crime legislation.¹⁶⁹

136. RECOMMENDATION

Abuse targeted at female MPs and candidates remains a particular issue. Sex remains the only protected characteristic not covered by the protections of hate crime legislation or aggravating factors at sentencing. The debates around how hate crime legislation might cover misogynistic abuse of this kind are complicated and could have significant impact on women across the country. The Government should review the findings of the Law Commission, as well as the Scottish and Northern Irish studies, about making misogyny an aggravating factor. The political parties should recognise that the challenge of misogynistic abuse is unlikely to be resolved soon or easily and offer tailored support to their female officials and candidates to reflect the additional pressure they are likely to be under.

137. RECOMMENDATION

In our first report we recommended that police forces should plan for “the potentially higher risk profile some candidates may have, either carried over from their time as an MP, because of their own prominence, or for other factors affecting their level of risk, whilst ensuring no political advantage is given to any candidate”: for the sake of clarity we confirm that this should include considering the greater risks of abuse and intimidation female candidates are likely to face, especially online.

Electoral disqualification orders

- 138.** In our first report, we said we would “return to the question of whether current legal restrictions on standing for election are sufficient”. Our first report identified a particular issue with data gaps around the implementation and effectiveness of the disqualification orders introduced by the Elections Act 2022, which bar people convicted of intimidatory

¹⁶⁸ [Qq257–258](#)

¹⁶⁹ Scottish Government, [Misogyny – A Human Rights Issue](#), 8 March 2022, p 12; Hate crime legislation in Northern Ireland Independent Review, [Final Report](#), p230

offences from standing for election for five years.¹⁷⁰ We recommended that the Government monitor the use of disqualification orders and report the results to Parliament and the Speaker's Committee on the Electoral Commission in time for any necessary reforms to be made before the next election.¹⁷¹

- 139.** The evidence we have heard since then about how disqualification orders are imposed has been worryingly inconsistent. The Crown Prosecution Service and the then-Solicitor General told us that in cases where the criteria for making a disqualification order are met, a prosecutor would not apply for one as the court must make one unless it is unjust to do so.¹⁷² However, Lord Colbeck told us that, because the orders are new and “a little bit niche”, “[t]he availability of a disqualification order would probably have to be drawn to the court’s attention, if it was being sought”.¹⁷³ Nick Price did seem to indicate that prosecutors might more proactively seek disqualification orders on a case by case basis and that the orders are handled by a specialist team in the Special Crime Division.¹⁷⁴ There are worrying indications that courts are regularly omitting to make these orders: in six recent cases where an order should have been imposed, the then-Solicitor General told us that none were, no reasons were given by the courts for the omission and CPS records do not identify whether disqualification orders were considered.¹⁷⁵ At least one CPS regional unit has already reminded its prosecutors that these orders should be applied, after the court failed to impose one in a local case of criminal damage against an MP’s office.¹⁷⁶

170 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 34. Intimidatory offences include assault, public order and sexual offences, and harassment. A disqualification order is imposed if the offence is shown to have been motivated by the fact the victim was an election candidate or campaigner. (House of Commons Library, “[Intimidation of candidates and voters](#)” Research Briefing 9192, 28 July 2025)

171 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 37

172 Letter from Lucy Rigby KC MP, Solicitor General, to the Chair regarding evidence given to the Conference on 2 July 2025, [8 August 2025](#); Letter from Director of Public Prosecutions to the Chair regarding the work of the Speaker’s Conference, [9 May 2025](#); [Q262](#) [Lucy Rigby KC MP]

173 [Q218](#)

174 [Qq221–223](#); Letter from Lucy Rigby KC MP, Solicitor General, to the Chair regarding evidence given to the Conference on 2 July 2025, [8 August 2025](#)

175 Letter from Lucy Rigby KC MP, Solicitor General, to the Chair regarding evidence given to the Conference on 2 July 2025, [8 August 2025](#)

176 [Q263](#) [Lucy Rigby KC MP]

140.

CONCLUSION

When individuals are convicted of political intimidatory offences, the courts are required under the Elections Act to impose electoral disqualification orders, which bar them from standing for relevant elected roles for five years. There is a worrying lack of awareness and understanding about electoral disqualification orders, and indications that courts may be consistently omitting to impose them. Although these really affect only the small number of perpetrators who might wish to stand for election, the confusion around them reflects a lack of care and prioritisation of an important issue: the ability to stand for election is a valuable democratic right, and when it has been forfeited there must be certainty that that penalty will be consistently imposed to avoid any inequity or uncertainty about whether a candidate can stand.

141.

RECOMMENDATION

Before the Government carries out the review we have recommended of the effectiveness of disqualification orders, it should take immediate measures to ensure they are actually being used. The Crown Prosecution Service should instruct prosecutors to inform courts of their powers to use a disqualification order whenever relevant. The Sentencing Council, Scottish Sentencing Council and Court of Appeal in Northern Ireland should ensure that judges are aware of these orders, by updating sentencing guidelines, guideline judgements or guidance as appropriate. The Government should confirm in its response to this report that these steps have been completed or action taken to complete them within the next year.

3 Social Media

Introduction

- 142.** In our first report we concluded, based on a strong consensus of the evidence we received, that “The nature and tone of engagement on, as well as policies and approaches of some social media platforms, are contributing to the level of threats against MPs and candidates.”¹⁷⁷ In this chapter we consider what role social media plays in the UK’s democratic system, how the decisions made by the platforms themselves affect the ability of MPs and candidates to use their sites safely, and the adequacy of the legislation governing social media.

The role of social media in UK politics

- 143.** Social media is now an established part of the political process. Large numbers of MPs and candidates engage with constituents and voters on social media platforms, particularly Facebook, X, Instagram and WhatsApp. In our survey of MPs, 97% of respondents told us that they are active on Facebook, and 91% on X, as shown in the chart below. Some political parties now require their candidates to use social media as part of their campaigns.¹⁷⁸ Professor Patrícia Rossini, Professor of Political Communication, University of Glasgow, noted how integral social media has become: “it is hard to envision an election taking place with social media not being a part of it. It is hard to envision your work as politicians and communicating with the public in a world where these platforms no longer exist.”¹⁷⁹
- 144.** However, not all social media platforms play the same role in the political process. Professor Helen Margetts, Professor of Society and the Internet, Oxford University, stressed that social media use is not uniform and platforms can have different functions depending on how they are designed

177 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, paras 19–20

178 Online Safety Act Network ([SCS0001](#)); Dr Emily Harmer (Senior Lecturer in Media at University of Liverpool); Dr Rosalyn Southern (Senior Lecturer in Political Communication at University of Liverpool) ([SCS0017](#))

179 [Q306](#); The Center for Countering Digital Hate (CCDH) agreed that “social media has revolutionised politics” and is one of the main places for debate and discussion ([SCS0028](#))

and how users, including MPs and candidates, choose to engage on them. A social media platform can be a broadcasting tool or a way to engage directly with people and “[i]t may be that there are different channels for different things.” She also noted that a platform’s role can change over time, citing the example of how X has become less used as a public sphere for direct engagement in recent years.¹⁸⁰

- 145.** In turn the level of abuse can vary significantly between platforms based on how they are used.¹⁸¹ As shown in the chart below, our survey found that MPs were significantly more likely to have experienced abuse on X (81%) and Facebook (77%) compared to Instagram (15%), despite the fact that similar numbers of respondents reported being active on the three platforms.¹⁸² We have been told that the design of a platform affects the levels of abuse users experience, and that abuse is more likely if: a platform’s content is generally public (as opposed to shared only with known contacts e.g. on WhatsApp),¹⁸³ the platform is used for sharing text rather than images or videos, comments and responses to posts are prominently displayed, or the site already has a lot of abusive content.¹⁸⁴

180 [Q88](#)

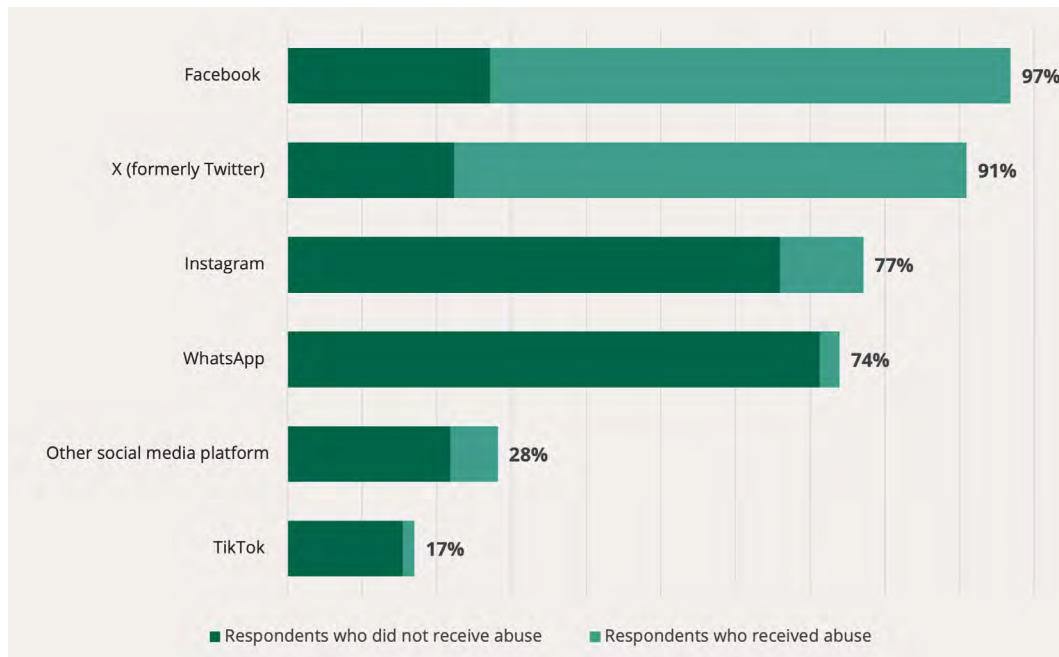
181 [Q88](#) [Professor Margetts]

182 Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, Annex 1 This is not to imply there is no problem with abuse on other platforms: although the percentage of respondents reporting abuse on WhatsApp was among the lowest, Rushanara Ali MP noted the use of the platform to spread threatening videos as a particular issue ([Q167](#))

183 [Q277](#) [Clair Dilé]

184 [Q278](#) [Prof Patrícia Rossini]

Chart 1: Percentage of MPs who are active on social media platforms, and the proportion of those active who have and have not received abuse on those platforms.



- 146.** The social media companies we spoke to, and who operate the platforms most used by MPs, do not think their platforms have a specific political function. X and Meta¹⁸⁵ both acknowledged that their platforms are useful to discuss public policy, that many people use them for that purpose, and that many MPs use them to communicate with constituents. However, they told us that they regard politics as one topic that users may wish to discuss on the platform, exactly the same as sport, entertainment or others.¹⁸⁶ Meta have even said that they are working to “reduce the amount of political content people see in Feed and recommendations” on Facebook and Instagram as users have said they want to see less political content.¹⁸⁷
- 147.** However, treating political discussions as equivalent to other topics discussed on a social media platform runs contrary to the platforms’ own perception of what triggers abuse online. Meta indicated that political discussions generated more abuse on social media than other topics, suggesting that the fact Facebook is regularly used for political

¹⁸⁵ In this chapter we refer to Meta in its capacity as the parent company for Facebook, noting that the issues we are considering are less prevalent on Instagram, another platform it operates which is similarly used by MPs and candidates.

¹⁸⁶ [Q272](#) [Clair Dilé, Megan Thomas]

¹⁸⁷ Written evidence received by the Science, Innovation and Technology Committee’s inquiry into Social media, misinformation and harmful algorithms, Meta ([SMH0037](#)), 22 January 2025

conversations might be one reason why MPs receive significantly more abuse on the platform than on Instagram (which they told us is used for “lifestyle conversations”).¹⁸⁸

148. CONCLUSION

Social media platforms can be useful tools for MPs and candidates, and we anticipate that the part they play in facilitating engagement with constituents and voters is here to stay. However, these platforms are all private commercial products and are not designed or operated to have a specific political function. As such they form no part of the Fourth Estate, which we have acknowledged in Chapter One is a core pillar of democracy, and have no constitutional role. The impression held by some people, including some MPs, that MPs are required to make themselves available to their constituents on social media platforms is entirely false. MPs have as much right to decide who they and their staff engage with online as in person or by other means, and there is no requirement or convention for an MP to use a social media platform to send or receive communications. Moreover, unless there is a radical change in how social media companies treat political conversations and users, no such convention should be allowed to evolve.

149. CONCLUSION

Currently only a few social media platforms are regularly used by candidates and MPs for their work, and, of those that are, the levels of abuse on the platforms vary significantly. We have therefore paid particular attention in the remainder of the chapter to the social media platforms that are the main source of threats to MPs and candidates: Facebook and X. However, patterns of social media use are likely to change, especially if the platforms fail to keep users safe from abuse, and we therefore encourage other social media platforms to learn from the lessons we have identified, in particular the greater risk of abuse faced by political figures and the greater care that must be taken to prevent it.

Abuse on social media

- 150.** 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 Parliamentary Security Department (PSD) told us that 83% of security incidents occur by virtual means, such as social media or email.¹⁸⁹ In our survey of MPs, over 90% of those who had experienced a threat had experienced it online, with many fewer reporting having

188 [Q276](#) [Megan Thomas]

189 Parliamentary Security Department ([SCS0045](#))

experienced a threat in-person (33%-67% depending on the type of threat). MPs' staff are often on the frontline of online abuse: over two thirds of MPs who said they have an active social media presence in response to our survey also said that they delegate management of their accounts to staff. The ongoing development of Artificial Intelligence is expected to "turbocharge" these issues and other online harms. But AI will also play an important role in tackling these issues, including its own malicious use.¹⁹⁰

151. Although thankfully it is rare for online threats to translate into physical risk, the two are not unrelated. In Chapter 1, we outlined concerns that the prevalence of abuse online was habituating people to more aggressive and abusive exchanges, which they were carrying through to their offline interactions. The impact of online abuse can also directly spill into the offline world,¹⁹¹ particularly when images or videos of in-person abuse are shared on social media: this footage can generate further abuse online and offline, stirring up others to abuse MPs and candidates in the same way. Often this is deliberate, with individuals harassing candidates or campaigners in-person so that the incident can be filmed and shared online.¹⁹²
152. Female MPs and candidates, and those from ethnic minority backgrounds, face particular and heightened online threats, receiving significantly more abuse than their white, male counterparts.¹⁹³ Precisely how much more abuse women and politicians from ethnic minorities receive, and why, is challenging to measure because of the many factors that influence the amount of abuse individuals receive online, including how often they post and how prominent they are.¹⁹⁴ However, witnesses have noted that women consistently receive a disproportionate amount of sexualised abuse, and disproportionately high abuse if they become more prominent or senior in a party, while politicians from ethnic minorities receive a disproportionate amount of hate speech. Female ethnic minority candidates "faced

190 [Q95](#) [Prof Helen Margetts]; The way that AI has heightened vulnerabilities in democratic systems, as well as the immense benefit it can bring, was also noted in the Declaration of the 23rd Meeting of the Speakers of the Lower Houses of the G7 (Appendix 1)

191 [Q29](#) [Elfrede Brambley-Crawshaw]; [Q78](#) [Prof Helen Margetts]

192 [Q45](#) [Vijay Rangarajan]; [Q159](#) [Rushanara Ali MP]

193 [Q78](#) [Professor Margetts]

194 [Q78](#) [Professor Margetts]; Reset.Tech told us that the female politicians in their study received more abuse because they posted more and received more engagement both positive and negative ([SCS0004](#)). Researchers identified the factors influencing the levels of abuse MPs and candidates receive on social media as: their prominence, their personal characteristics, such as gender or race, the general level of engagement they have online, and events that draw attention to them (Dr Diana Maynard (Senior Research Fellow at University of Sheffield); Professor Kalina Bontcheva (Professor at University of Sheffield) ([SCS0014](#)); Florence King (PhD Researcher at Swansea University) ([SCS0015](#)))

significantly more hate speech than their male counterparts, underscoring the compounding impact of discrimination based on both ethnicity and gender.”¹⁹⁵ Worryingly, the issue of misogynistic abuse is getting worse.¹⁹⁶

The role of social media platforms

- 153.** Experts have told us that the problem of abuse on social media is compounded by the platforms’ decisions about what content they will permit or promote on their platforms. Despite the fact that X and Meta both told us that they expect users to comply with their policies on what content is acceptable and have mechanisms for reporting content that contravenes these policies,¹⁹⁷ we have been told that the social media platforms have become increasingly unwilling to remove abusive content. Part of PSD’s role is to report online threats against MPs to the relevant social media platform for removal: they tell us they have “twice changed [their] thresholds for referring messages to social media platforms due to the high proportion of abusive messages not being taken down. [PSD] now routinely refer only directly threatening and grossly offensive material to platform[s], as [they] know this is the only material that will be considered for removal.”¹⁹⁸ Oliver Davis, Deputy Director (Members’ Security and Risk), Parliamentary Security Department, told us that while platforms have previously been willing to work with PSD to remove abusive and intimidating content, they no longer have “any interest whatsoever.”¹⁹⁹
- 154.** As well as the platforms’ decisions about what content to remove, another issue is their choice of what content to recommend to users, for example on home pages or in feeds. The Center for Countering Digital Hate and Glitch, a charity that addresses online harms, both argued social media platforms have a financial incentive to promote incendiary and divisive content because it attracts and retains users’ attention on the platform, increasing advertising revenue.²⁰⁰ Meta and X both denied that their platforms actively promote harmful content for commercial reasons, telling us that their advertisers did not wish to be associated with content that was harmful

195 Reset.Tech ([SCS0004](#)); Dr Diana Maynard (Senior Research Fellow at University of Sheffield); Professor Kalina Bontcheva (Professor at University of Sheffield) ([SCS0014](#)); [Q78](#) [Professor Margetts]

196 [Q355](#) [Jessica Zucker]

197 [Qq274–275](#) [Megan Thomas]; [Qq 273, 281](#) [Claire Dilé]; Meta ([SCS0054](#)); X (formerly known as Twitter) ([SCS0055](#))

198 Parliamentary Security Department ([SCS0045](#))

199 [Q143](#)

200 Center for Countering Digital Hate (CCDH) ([SCS0028](#)). Glitch raised similar concerns about a financial incentive to prioritise “sensational and divisive” disinformation ([SCS0018](#)). BCS (The Chartered Institute for IT) also noted concerns about users having a financial incentive to post divisive material ([SCS0025](#))

or illegal.²⁰¹ However, Professor Rossini suggested that incendiary content might be promoted without a direct financial motivation: she said that because most social media platforms suggest or recommend content based on the amount of engagement it has had, negative engagement with a post appears to increase the chance that it will be recommended. This could lead to “this toxic spiral of hate whereby abusive comments attract more abusive comments.”²⁰² We discuss in more detail how platforms promote content and the challenges in understanding the role played by their recommendation algorithms below.

Protections for users

- 155.** There are ways that users can try to reduce the amount of abuse they receive. Each platform offers different functions, but common or notable strategies raised during this inquiry include:
- blocking other users who persistently engage in abuse or intimidation;²⁰³
 - hiding or deleting abusive comments;²⁰⁴
 - reporting abusive posts;²⁰⁵
 - reducing the use of platforms where abuse is common, and finding alternative platforms;²⁰⁶
 - using a “broadcast mode” of communication by posting but not responding to replies (and making this approach clear on the relevant profile).²⁰⁷
- 156.** Additionally, once they are fully implemented, sections 64 and 65 of the Online Safety Act 2023 and the accompanying guidance from Ofcom will require the largest platforms to give users the option to verify their identity, giving users the ability to filter out content from non-verified users.²⁰⁸ Ofcom told us that they are still considering exactly what the measures around

201 [Q308](#) [Megan Thomas, Clair Dilé]

202 [Q278](#) Professor Helen Fenwick also told us that more controversial content on social media generated more attention and encouraged others to also engaged aggressively online ([Q210](#))

203 Dr Emily Harmer (Senior Lecturer in Media at University of Liverpool); Dr Rosalynd Southern (Senior Lecturer in Political Communication at University of Liverpool) ([SCS0017](#))

204 As above

205 As above

206 Reset.Tech ([SCS0004](#))

207 Dr Emily Harmer (Senior Lecturer in Media at University of Liverpool); Dr Rosalynd Southern (Senior Lecturer in Political Communication at University of Liverpool) ([SCS0017](#)); Reset.Tech ([SCS0004](#)); [Q88](#) [Prof Helen Margetts]

208 [Online Safety Act 2023](#) ss 64–65

anonymous accounts will look like and that in addition to the ability to block non-verified accounts they are also considering requirements such as ensuring content from these accounts appears only at the bottom of comment threads, limiting the type of interactions people can have with a user, or displaying warning screens over some content, so that users, particularly public figures, can still maintain some awareness of potential threats if needed.²⁰⁹

- 157.** These provisions about unverified accounts respond to concerns that anonymity enables online abuse, particularly criminal incidents of harassment, stalking and violent threats.²¹⁰ Several witnesses warned that the effect of restricting anonymity online on abuse might be limited. A large amount of abuse comes from accounts displaying the user's real name and personal details, indicating that anonymity may be a less significant factor in encouraging abuse than a perceived lack of consequences for online activity.²¹¹
- 158.** Using protective measures like these can be effective: Reset.Tech, an international charity addressing digital threats to democracy, told us the protective measures taken by Diane Abbott MP's office had significantly reduced the number of threats she received from "historically high levels of social media abuse" to "the lowest threat count among female politicians".²¹²
- 159.** However, several witnesses have also warned strongly against relying on MPs and candidates to protect themselves from social media abuse. Florence King, a PhD researcher at the Cyber Threats Research Centre, told us "Candidates and MPs should not be expected to alter their social media usage ... to mitigate online harms. Advising individuals to disengage from social media in response to harassment is deeply problematic, as it normalises abuse, implies its inevitability, and shifts responsibility from perpetrators to victims."²¹³ Other evidence noted that using protective measures reduced an MP or candidate's engagement on a platform, forcing them to try and balance their safety and their campaign, and that this trade off particularly affected women and people from ethnic minority backgrounds, as those most at risk of abuse.²¹⁴

209 [Q357](#) [Jessica Zucker]

210 Clean up the Internet ([SCS0007](#)); Professor Helen Fenwick also suggested that many threats came from anonymous accounts ([Q210](#))

211 [Q199](#) [Elisabeth Costa]; [Q312](#) [Claire Dilé]; [Q317](#) [Prof Patrícia Rossini]

212 Reset.Tech ([SCS0004](#))

213 Florence King (PhD Researcher at Swansea University) ([SCS0015](#))

214 Professor Susan Banducci (University of Birmingham) et al. ([SCS0030](#)); [Qq 78, 84](#) [Professor Margetts]; [Q306](#) [Prof Patrícia Rossini]

160. CONCLUSION

The benefits social media bring to political engagement come at the significant cost of innumerable online threats against MPs and candidates. It falls disproportionately on female and ethnic minority politicians, who are more likely to be abused online relative to their white, male counterparts. The cost continues to rise, as social media platforms tolerate more and more content that would previously have been deemed unacceptable under their terms of service. Whilst MPs and their staff pay the price directly, everyone is indirectly affected because of the damage online abuse is doing to political discourse. The development of Artificial Intelligence will only compound these costs, while at the same time being a necessary tool for addressing the issue.

161. RECOMMENDATION

Although individual MPs and candidates do not have the power to solve the problem of online abuse, to keep themselves and their staff safe, and to preserve the quality and civility of online discourse, they should all actively engage the protective tools available to them on the social media platforms they use, such as ignoring or restricting replies and automatic filtering of offensive language. Additionally, they should block, screen or filter content from accounts that have not verified their identity, once this function is implemented under the Online Safety Act 2023. They should act swiftly to block any users, including constituents, who they feel are engaging in an abusive or aggressive manner. By reducing opportunities for individuals to post abusive and intimidatory content online, MPs and candidates will help to defuse the “toxic spiral of hate” that drives ever more abuse, exposes other users on the platform to inappropriate and distressing content, and dissuades people from standing for public office.

162. RECOMMENDATION

MPs and candidates should feel empowered to leave any platform they judge to present a greater risk than benefit to their work. If political parties require candidates to post on specific social media platforms they should assess the risks and benefits of doing so for each individual candidate, carefully considering the political and personal factors that affect the chance the candidate will be abused.

163. CONCLUSION

Relying on MPs and candidates to protect themselves on social media places a greater burden on groups more at risk of abuse, typically women and politicians from ethnic minority backgrounds, and can make it harder for them to campaign by reducing their engagement with the public. To avoid an unintentional discriminatory effect, it would be best if all MPs and candidates use all the protective measures available to them boldly and consistently.

164. CONCLUSION

Although we encourage MPs and candidates to use the available tools to counter abuse, this will only go so far. For as long as people continue to use social media as a mouthpiece for abuse, true responsibility for resolving the issue of threats on social media lies with the platforms that host them.

Meta's and X's response to abuse

- 165.** Meta and X told us that they take abuse of MPs and candidates seriously and that they recognise a duty to keep their users safe. X told us that they “have a responsibility at all times” and “it is very important that people who use the platform are not victims of abuse.”²¹⁵ Meta told us twice that they have “a responsibility to balance freedom of expression with the safety of [their] users” and that they “absolutely recognise the importance of the Conference’s work to date on this issue.”²¹⁶
- 166.** However, their engagement with our inquiry has caused us to doubt their sincerity. Meta and X chose to send relatively junior witnesses²¹⁷ who at times struggled to answer questions, particularly regarding important policies like the evidence X requires from the police before the platform will share information²¹⁸ and how Meta assesses the credibility of threats made on their platforms.²¹⁹ The follow up evidence they provided in writing was often more evasive than it was informative: for example, when Meta was

215 [Q275](#) [Claire Dilé]

216 [Qq272–274](#) [Megan Thomas]

217 X and Meta were both invited to send the representatives they felt most appropriate. They sent the Government Affairs Director, Europe, and a Public Affairs Manager respectively. By way of contrast when invited to give evidence to the Science, Innovation and Technology Committee they sent the Senior Director for Government Affairs and the Director of Public Policy for Northern Europe (Oral evidence taken by the Science, Innovation and Technology Committee on 25 February 2025, [Qq 88–179](#)). When invited to give evidence to the Senate Judiciary Committee in the United States in January 2024 they sent their CEOs (The Drum, “[5 key takeaways from Meta, TikTok, X, Snap’s Congressional hearing on kids’ online safety](#)”, 31 January 2024).

218 [Qq286–288](#) [Claire Dile]

219 [Qq303–305](#) [Megan Thomas]

asked for their target times for removing abusive content they took four paragraphs to tell us that speed of removal depends on “a range of factors”, and when asked for the percentage of requests for information from the police they had denied due to insufficient evidence to support the request, X declined to say.²²⁰

Mitigations

- 167.** Meta and X have both put in place some measures to mitigate the abuse related to MPs and candidates, such as specific escalation routes for the Parliamentary Security Department to report abusive content,²²¹ but much of their work is focused on elections. X and Meta both told us that during election periods they proactively sweep their platforms for relevant violations of their policies.²²² They also establish mechanisms to work with candidates and parties. X has an email address for political parties to report violations of terms of service, or other issues related to the election.²²³ Meta seem to go further, telling us that they work directly with candidates, digital officers or other points of contact for all political parties represented in Parliament.²²⁴
- 168.** These election-specific measures were welcomed by many political parties, but smaller parties told us they did not receive the same support from Meta and X and find it challenging to raise issues with them. They argued strongly that they should be able to engage directly with the same named contacts at the social media companies, and suggested that it might enable them to resolve many of the worst instances of abuse before they spiralled further.²²⁵
- 169.** Outside elections, Meta told us that one of the measures they have implemented to address abuse against any users on Facebook and Instagram is automated prompts or “nudges” that remind users about appropriate content in situations where a post may be abusive. Meta told us these nudges, which they say have been effective on their platforms, are used if the content of a post may be considered offensive, if the post is contributing to a heated comment thread, or when a message is being sent directly to “creators” (a type of professional account).²²⁶
- 170.** We have heard strong evidence in favour of using nudges like these to address abuse. Elisabeth Costa told us that they give users a chance to reflect and break the “hot state decision making” (decisions made in a

220 Meta ([SCS0054](#)); X (formerly known as Twitter) ([SCS0055](#))

221 [Qq274–275](#) [Megan Thomas]; Meta ([SCS0054](#))

222 [Q275](#) [Claire Dilé, Megan Thomas]

223 X (formerly known as Twitter) ([SCS0055](#))

224 Meta ([SCS0054](#))

225 [Q44](#) [Owen Roberts, Colin McGrath]

226 Meta ([SCS0054](#))

state of strong emotion) that appears to be responsible for a large amount of abusive content online. Research has shown that nudges inviting users to revise posts that may be offensive lead to a significant number of posts being revised or not posted at all and also helped improve the civility of engagement on the platform more widely.²²⁷ In 2020, X (then Twitter) introduced these kinds of automated prompts after finding they led to a significant decrease in abuse,²²⁸ although in their written evidence X told us that the platform “does not use automatic prompts asking users to reconsider before making any posts.”²²⁹

171. CONCLUSION

Although Meta and X’s engagement on this issue during this inquiry has raised serious questions about their sincerity and determination to tackle it, they have recognised that they have responsibilities to their users and to democracy and are putting in place measures to mitigate abuse. These should be welcomed and expanded. In particular, Meta must engage better with smaller parties and offer them the same direct engagement enjoyed by the larger parties. X provides a generic email address to the Electoral Commission to be shared with parties and candidates: it would be more effective for them to use the same model as Meta of a central liaison with parties. X should also return to its old policy, currently still used by Meta, of deploying automated messages to warn people when the content they are about to post may be abusive and contrary to the platform’s policies. These nudges should be used more widely. For example, similar messages to those that users receive when they engage with creators on Facebook should also be used when contacting MPs or other elected officials, telling users that they are about to contact an elected representative, noting the importance of free speech and robust debate, but warning that threats and abuse undermine democracy, make it harder for politicians to represent their constituents, and are often illegal.

- 172.** Elisabeth Costa also suggested that Parliament consider implementing a similar automated prompt system for its email system.²³⁰ This could have a significant impact, as a review of threatening communications reported to the Parliamentary Security Department showed that the majority were sent by email.²³¹ Unfortunately, the Parliamentary Digital Service informed us that there are technical limitations on implementing this approach on an email system. They told us that Parliament already offers MPs the option to opt-in

227 [Qq 199, 211](#); Behavioural Insights Team ([SCS0052](#))

228 Behavioural Insights Team ([SCS0052](#))

229 X (formerly known as Twitter) ([SCS0055](#))

230 Behavioural Insights Team ([SCS0052](#))

231 Parliamentary Security Department ([SCS0045](#)) The review covered security incidents reported to PSD in Q4 2024.

to having emails that contain certain types of offensive language filtered. Filtered emails can be held so the recipient never sees them, or the recipient is shown the sender and subject before deciding if they wish to see the full message. They told us it would also be possible to tag filtered emails with labels letting the recipient know that they may contain abusive content. However, it is not possible to return filtered emails to the sender with the option to send it unchanged and for that message to not be repeatedly filtered and returned to the sender. They did tell us that there may be other alternatives to email, such as adopting the use of contact forms for each MP on the Parliamentary website. A range of similar options, such as communication portals or gateways are already being introduced by other legislatures and similar organisations.²³² Such alternatives may make it possible to check whether a message contained abusive content, and invite the sender to revise it, as well as to check whether it contained necessary information for contacting an MP, like the sender's postcode.²³³

232 Westminster Foundation for Democracy, [A new communication portal for the Moroccan Parliament](#), 3 July 2020 (accessed 23 September 2025); UNHCR, [Digital Gateway](#), unhcr.org (accessed 23 September 2025)

233 Letter from the Managing Director, Parliamentary Digital Service, to the Chair regarding abuse received by Parliamentary email accounts, [8 September 2025](#)

173.

RECOMMENDATION

As much of the abuse MPs receive comes through the Parliamentary email system, Parliament should explore whether to introduce automated prompts asking users to reconsider potentially abusive messages. As part of this exploration, the Parliamentary Digital Service (PDS) should consider alternatives to email, such as moving to an online contact form for MPs, as is the model in other legislatures, or systems such as contact portals or gateways, which could allow two-way dialogue between recipient and sender. These approaches could allow for the introduction of a prompt when people try to submit a potentially threatening message, inviting them to reconsider, while still allowing them to send the original message if they wish to. As part of its exploratory work, PDS should consider whether such an approach would make it easier: to process and screen messages for abusive content, to ensure messages are directed to the correct MP, to improve ability to manage the increasing volume of email received by MPs, and to implement the kind of behavioural nudge described above. It must consider that constituents' messages will often contain heightened emotional language which is expressive not threatening, and how to preserve the important human aspect of the nature of communications between MPs and their constituents. Any change of approach should be balanced with the need to maintain appropriate filtering, anti-spam and security measures, digital accessibility and MPs' offices' autonomy to manage responses and casework. Any proposed solution should be informed by clear political direction and consensus, with MPs being consulted as part of the development of any new system. Proposals should be presented to the House of Commons Administration Committee in time for consideration ahead of the next Parliament.

174.

RECOMMENDATION

In the meantime, PDS should work to increase awareness among MPs of the current optional facilities for screening emails for abuse and consider introducing banner-style messages for recipients on emails received containing potentially abusive content, signposting to appropriate reporting and support mechanisms.

Broader safety measures

- 175.** Despite having put some mitigations in place, neither Meta nor X recognise that the companies' decisions on fundamental elements of how their platforms work contribute to the spread of abuse.

Tolerance for political abuse

- 176.** We noted above that despite telling us they have policies on acceptable content in place, and mechanisms for users to report violations, Meta and X appear to be increasingly unwilling to take down abusive or intimidatory content. What is more, both platforms have an even higher tolerance for abusive content that targets politicians and other public figures, despite the fact that researchers have told us that a higher bar leads to higher levels of abuse against those affected,²³⁴ specifically: X’s decisions on enforcement action against posts that breach their terms of service include considering whether “[t]he content may be a topic of legitimate public interest”;²³⁵ and Meta’s policy is only to remove violent threats against public figures, such as MPs and candidates if they are found to be “credible”. Although Meta told us this assessment is “a complex process based on multiple factors”, their description of the credibility test indicates that they impose a high bar when considering whether a threat of violence against an MP is credible, for example by looking for specific locations and timing of a potential attack.²³⁶
- 177.** Meta and X justified some of this reluctance to remove threats against MPs and candidates by saying that it is not obvious whether posters intended comments to be taken as threats. X told us that it is necessary to understand the context behind a post when assessing whether it breached their policies.²³⁷ Meta told us that one of the particular issues they often have to consider in determining if a post constitutes a threat is whether a user is employing a “turn of phrase”.²³⁸ Adding to the challenge of understanding the true meaning behind a comment, is the fact that there appears to be an increasing tendency to use hyperbolically negative language in political debate to get public attention or make a point.²³⁹
- 178.** Understanding the context behind a post is challenging and cannot be achieved by automated systems alone. Jessica Zucker, Director of Online Safety Policy, Ofcom, said that based on her experience of working in the technology sector before joining Ofcom, platforms needed to have human moderators for a content moderation system to function, along with automated features.²⁴⁰ X confirmed that because understanding hateful content depends so much on context, they do rely on human agents to

234 Dr Diana Maynard (Senior Research Fellow at University of Sheffield); Professor Kalina Bontcheva (Professor at University of Sheffield) ([SCS0014](#))

235 X, [Global Transparency Report H1 2024](#), transparency.x.com, p3

236 Meta, [Community Standards: Violence and incitement](#), transparency.meta.com (accessed 24 September 2025); Meta ([SCS0054](#))

237 [Qq 280, 291](#) [Claire Dilé]

238 [Qq297–298](#) [Megan Thomas]

239 Professor Alan Renwick (Professor of Democratic Politics and Deputy Director of the Constitution Unit at University College London) ([SCS0031](#))

240 [Q362](#)

review such posts.²⁴¹ We were therefore surprised when X told us that they have only 1,486 human reviewers working in English, especially since figures provided by the company indicate they receive more than 85,000 posts that breach their terms of service every day.²⁴²

- 179.** However, we also heard concerns that too much emphasis could be placed on whether or not a threat is credible. Professor Rossini told us that she was not convinced that the platforms would be able to properly assess the credibility of threats and stressed that even abusive comments that were not intended as true threats cause a significant amount of harm: “If we consider the issues from the victim and target standpoint, and consider not just the anxiety and stress but also the downstream consequences in terms of politics and participation and engagement in politics, and even in continuing to work in politics, we really need to consider these issues from more of a, “Does it matter if it’s credible?” standpoint”.²⁴³ Ofcom also told us that the companies’ obligations to remove illegal content, such as threats to kill or harm, required them to have reason to believe that the content was illegal, but not to have evidence of the mental state of the user that posted it.²⁴⁴ They also stressed that platforms could not set their own bars for removing illegal threats.²⁴⁵

Resisting police requests

- 180.** Even when abuse crosses the criminal threshold, X appears to be unwilling to act. We raised concerns that, when individuals were prosecuted for posts, they remained on the platform, and that when police request information about the identity of individuals who have posted content as part of an investigation, X often did not provide it.²⁴⁶ X told us that they do remove illegal content when notified of it. However, in the latest six-month period the company shared information with the police in less than half of the instances when it was requested formally, and in only 30% of instances when it was requested informally.²⁴⁷

241 [Q280](#) [Claire Dilé]

242 X told us they receive 500 million posts a day (in all languages), of which 0.017% are in violation of their policies ([Q277](#) [Claire Dilé]; X (formerly known as Twitter) ([SCS0055](#))

243 [Q317](#)

244 [Qq352–354](#); As outlined in more detail below, the Online Safety Act introduced a legal requirement for social media platforms to have systems to remove content that was against the law, for example a threat to kill.

245 [Q378](#) [Mark Bunting, Almudena Lara]

246 Sometimes the platform will hold information related to anonymous accounts that is not publicly available, such as IP addresses.

247 [Qq283–288](#) [Claire Dilé]; X (formerly known as Twitter) ([SCS0055](#))

181. X told us that any formal requests for information had to be made in line with the terms of a Mutual Legal Assistance Treaty (MLAT) or the UK-US Data Access Arrangement.²⁴⁸
182. In contrast, Meta told us that they also share information with the police under the US-UK Data Access Agreement, but that requests to them for subscriber information or IP addresses are typically made under the Investigatory Powers Act 2016. Meta provided data in response to 85% of the requests they received from police last year.²⁴⁹

Opaque algorithmic amplification

Box 1: Definition of algorithm

An algorithm is a “set of instructions a computer follows to perform tasks or solve problems. A recommendation algorithm is a type of algorithm designed to suggest data or content based on patterns in user behaviour or preferences. A social media recommendation algorithm selects and promotes content or accounts that it predicts will engage users, shaping individual feeds and influencing what users see, usually aiming to increase engagement and time spent on the platform.”

Source: Science, Innovation and Technology Committee, Second Report of Session 2024–26, [Social media, misinformation and harmful algorithms](#), HC 441, page 7

183. Not only are Meta and X reluctant to remove content that threatens MPs, but we have also heard concerns that when abusive content remains on the platform it is actively spread to other users. As noted earlier, social media platforms organise and prioritise content and there are indications that content that receives a lot of negative engagement is promoted and therefore amplified by the platforms’ recommendation algorithms, often triggering further abuse. Professor Rossini told us that it is challenging to understand whether and how abusive content spreads on a platform because how the algorithms operate is not transparent.²⁵⁰ She noted that researchers and regulators currently have to rely on the data the company is willing to share to assess whether abuse on platforms is getting better, which was akin to “asking children, “Did you eat the chocolate or not?”, and we have to trust that whatever they say they did is true, because there is virtually no way for independent researchers to verify any of these things.”²⁵¹

248 X (formerly known as Twitter) ([SCS0055](#))

249 Meta ([SCS0054](#))

250 [Q278](#)

251 [Q332](#)

- 184.** The Online Safety Act 2023 empowers Ofcom in the course of its regulatory duties to obtain information on a platform’s operations, including the algorithms it uses, and to require a regulated service provider to take steps so that Ofcom can remotely view information, including algorithms, in real time to show how its systems, processes or features work.²⁵² It also has transparency provisions to require platforms to share information with independent researchers.²⁵³ However, witnesses expressed doubt that the level of information provided would be sufficient.²⁵⁴
- 185.** Ofcom confirmed that they would have the power to request information on recommendation algorithms: they told us it would be “complicated and challenging to do”, although they expressed hope that recommendations in the codes of practice that platforms test the consequences of their algorithms would be important to show the scale of the issue and whether platforms were taking action.²⁵⁵ Ofcom did stress the potential for new requirements for the platforms to publish data, both under the transparency reporting functions and the provisions for the Secretary of State to create a researcher access data framework, to significantly improve research into how the algorithms work. Jessica Zucker called the framework “a real opportunity” and predicted that it would make a “huge difference” to UK researchers’ capabilities.²⁵⁶ Kanishka Narayan MP, Parliamentary Under-Secretary of State for Science, Innovation and Technology, confirmed that the Government is currently considering Ofcom’s report into existing access and barriers to research and its recommendations.²⁵⁷

252 [Online Safety Act 2023](#) s 100

253 [Online Safety Act 2023](#) s 154a

254 [Q332](#) [Prof Patrícia Rossini]; Glitch ([SCS0018](#)) argued that data on content moderation outcomes would need to be disaggregated by protected characteristics to be effective.

255 [Qq371–373](#) [Jessica Zucker, Mark Bunting, Almudena Lara]

256 [Qq 371, 381](#)

257 Letter from the Parliamentary Under-Secretary of State for Science, Innovation and Technology to the Chair regarding evidence to the Conference on 9 September 2025, [15 September 2025](#)

186. CONCLUSION

Despite the steps Meta and X have taken to mitigate some of the problems with abuse on their platforms, abusive content continues to be an issue. Their failure to address the larger underlying issues that drive abuse demonstrates that they do not properly understand the damaging impact they are having on democracy in the UK. We are particularly concerned about their unwillingness to remove abuse against MPs, candidates and other public figures; indications that X and Meta's algorithmic recommendation systems appear to give preference to incendiary and threatening content but with no recourse for independent review to assess this risk; and challenges the police and criminal justice system appear to face in obtaining information from X. We have no faith that Meta and X will resolve these issues unless they are legally obliged to do so. There is therefore no point in us recommending wholesale change of policies or modus operandi. The only viable solution is for Ofcom and the Government to compel them to protect their users. Currently, this will be via the Online Safety Act 2023. But should that legislation fail to tackle the root issues that influence the level of abuse and intimidation on social media platforms, further legislation will be needed. We return to this point in the final part of this Chapter.

187. CONCLUSION

Meta and X's greater tolerance for abuse against MPs, candidates and other public figures is a particular challenge. Both platforms are unwilling to properly assess and remove clearly inappropriate content; we doubt this is even possible for X given its disproportionately small content management team.

188. CONCLUSION

We agree that it can be hard to tell whether a threat made on social media against a public figure is real. Part of the challenge is that some threats may be used metaphorically or hyperbolically, but still add to a febrile political environment. We hope that the discussions between the Speaker, the parties and the Electoral Commission on a campaigning code of conduct will help to shape public understanding of the line where robust political discourse tips into inappropriately aggressive language.

189. CONCLUSION

However, taking refuge in this complexity, as platforms do, misses the point. Having higher bars for removing threats against politicians normalises the idea that MPs and candidates should be expected to endure a greater level of abuse than people in other professions: this impression puts people off running as candidates and is damaging democracy. Platforms' use of convoluted distinctions about whether a threat is "credible" or "severe" are an abdication of their responsibilities. We foresee the very real risk that these responsibilities will only be brought home to them in the worst way imaginable: when their assessment of the credibility of a threat is wrong, and they fail to remove content that instigates an attack.

190. RECOMMENDATION

The statutory requirement for platforms to remove illegal content covers threats against MPs, candidates and other public figures, just as much as anyone else. In order to ensure that these threats are properly dealt with, Ofcom should pay particular attention to whether platforms' content moderation procedures introduce additional criteria relating to the removal of illegal content related to public figures when it reviews them under the Online Safety Act 2023. They should specifically consider whether these additional criteria breach provisions of the Act around requirements for systems to remove illegal content and to enforce the platform's policies consistently. The Government should review the US-UK Data Access Agreement in consultation with the police to establish whether it is effective in granting police the access to information they need from social media platforms about criminal activities.

191. RECOMMENDATION

It is also important that, while abusive content remains on a platform, it is not promoted to other users, which can increase the harm to the victim and run the risk of triggering further abuse. The best defence against this is careful scrutiny of the platforms' recommendation algorithms by researchers and Ofcom. The Government should design and implement an access to data regime that delivers maximum transparency around platforms' operations.

The Online Safety Act and social media regulation

192. The primary legislative response to online abuse is the Online Safety Act 2023. This Act is still being implemented (as outlined in Box 2 below), and throughout this inquiry we have consistently heard the hope that it will have an impact on online abuse.²⁵⁸

Box 2: Summary of the Online Safety Act 2023

The Online Safety Act passed into law on 26 October 2023 and is being implemented in three phases:

- Phase 1 - Illegal content duties: came into force on 17 March 2025. Companies must now demonstrate to Ofcom that they have systems and processes in place to prevent, detect and remove illegal content from their platforms. The Act also lists “priority offences” such as terrorism, harassment, stalking, threats and abuse, and hate offences: for these offences social media companies must separately assess the risk of them occurring on their platform and take proactive measures to stop users encountering such content.
- Phase 2 - child safety duties: came into force on 25 July 2025.
- Phase 3 - additional duties for categorised services: still to be implemented. Certain platforms, to be determined by Ofcom, will have to comply with additional requirements. Depending on the size of the platform these will include annual transparency reporting, having to consistently enforce their terms of service, providing users with tools to avoid abuse targeting a protected characteristic, and steps to verify users’ identities and allow users to filter out content from non-verified accounts.

The Act makes provision for Codes of Practice developed by Ofcom and approved by the Government. Service providers need to adopt the safety measures set out in the Codes of Practice or use other effective measures to protect users. If they adopt all the measures set out in the Codes, they achieve “safe harbour” and are deemed compliant. Ofcom will be able to fine companies up to £18 million, or 10% of their global revenue (whichever is greater), if they fail to comply with their duties under the Act. In the most serious cases of non-compliance, Ofcom will be able to apply to the courts to block services in the UK. The Act does not empower Ofcom to direct the removal of individual pieces of illegal or harmful content.

258 [Q71](#) [Vijay Rangarajan]; [Qq 80, 84, 86](#) [Professor Margetts]; [Q201](#) [Professor Helen Fenwick]; [Q317](#) [Prof Patrícia Rossini]

The Act also creates new criminal offences, among which are two relevant communications offences which replace existing offences in the Malicious Communications Act 1988:

- Section 179 – False communications offence: A person commits the false communications offence if they send a message conveying information that they know to be false, and at the time of sending it they intend the message to cause non-trivial psychological or physical harm to a likely audience (i.e. someone who could reasonably be foreseen to encounter the message or its content) and they have no reasonable excuse for sending the message.
- Section 181 – Threatening communications offence: This offence criminalises the sending of a message conveying a threat of death, serious injury, rape, assault by penetration, or serious financial loss, and intends that (or is reckless as to whether) someone encountering the message will fear the threat will be carried out, whether by the sender or by others.

Sources: [Online Safety Act 2023](#); House of Commons Library, [Implementation of the Online Safety Act](#), Debate Pack, 25 February 2025; Department of Science, Innovation and Technology, [Online Safety Act: explainer](#), gov.uk, 24 April 2025 (accessed 24 September 2025); Ofcom, [Implementing the Online Safety Act: Additional duties for ‘categorised’ online services](#), ofcom.org.uk, 25 March 2024 (accessed 25 September 2025); Written evidence received by the Science, Innovation and Technology Committee’s inquiry into Social media, misinformation and harmful algorithms ([SMH0078](#)) footnote 3, 30 April 2025; Department of Science, Innovation and Technology, [Online Safety Act: new criminal offences circular](#), gov.uk, 31 January 2024, paras 30–34 (accessed 25 September 2025)

- 193.** As noted in Box 2 above, Ofcom writes the codes of practice that give practical effect to much of the Online Safety Act 2023. These codes of practice must be signed off by the Secretary of State and laid before Parliament. They are automatically approved unless Parliament passes a resolution to the contrary within 40 days of them being laid.²⁵⁹ Ofcom therefore has significant latitude for interpretation in the implementation of the Act: for example, it is Ofcom, rather than Parliament which will decide the services which will be subject to additional duties under phase 3. There are concerns that Ofcom has been too cautious in using the regulatory powers it was given, for example in not using powers to include smaller but riskier platforms among those subject to additional responsibilities.²⁶⁰

259 [Online Safety Act 2023](#), ss43–44

260 Online Safety Act Network, [Background briefing: House of Lords debate on OSA categorisation regulations](#), onlinesafetyact.net, 20 February 2025 (accessed 23 September 2025)

Clean Up the Internet argued that in response, Parliamentarians should find ways to demand faster progress from Ofcom and to counter any pressure put on the regulator by platforms to weaken the provisions of the Act in implementation.²⁶¹

- 194.** We asked Ofcom what they aimed to achieve in their implementation of the Act regarding threats against MPs and candidates. They expressed their ambition to achieve change in the social media industry’s culture, aiming for “commitment at the highest level [of] the companies that [they] are regulating to implement a more comprehensive approach to risk management”. They also noted the scale of the task, in particular, “the diversity and number of companies in scope of this regulation and the wide range of issues that Parliament has asked [them] to tackle.”²⁶²
- 195.** Ofcom told us they expected that the requirement for platforms to remove illegal content would cover a significant amount of the abuse politicians and others receive online. They said they “will not hesitate [to hold] platforms to account” to ensure they have terms of service that reflect these requirements, and content moderation systems that are effectively trained and resourced.²⁶³ The goal, they said, should be “earlier and proactive identification of this content, not waiting for users to report it and take it down.”²⁶⁴
- 196.** When it came to non-criminal abuse, Ofcom were more circumspect, as the Act does not require platforms to remove threats unless they break the law. However, they noted that the Act will require users on larger services to be given “additional tools to be able to choose what kind of content they see that might fall into this category of harmful but legal content.”²⁶⁵ They were optimistic that the platforms subject to the additional requirements under phase 3 would become more active at removing legal but inappropriate content. This would come from the improvements they would make to their content moderation systems to identify and remove illegal content, and the requirement that they consistently enforce their own policies on acceptable content.²⁶⁶

261 Clean up the Internet ([SCS0007](#)); Professor Fenwick also suggested Parliament should find ways to “to consider how the Online Safety Act could be made more effective and to call Ofcom to account” ([Q210](#)); The Center for Countering Digital Hate (CCDH) also called for the provisions of the Act to be strongly enforced ([SCS0028](#)).

262 [Qq385–387](#) [Mark Bunting]

263 [Q356](#) [Jessica Zucker]

264 [Q361](#) [Mark Bunting]. Meta and X both told us that they also aim to remove content proactively, before it is reported ([Qq307–308](#)).

265 [Q356](#) [Jessica Zucker] As we have noted above these include the ability to filter out abuse or hateful content that is related to a protective characteristic and to filter out content from non-verified users.

266 [Q362](#) [Mark Bunting; Jessica Zucker]

197. When asked if Ofcom faced any pressure to water down implementation of the Act, Mark Bunting, Director of Online Safety Strategy, Ofcom, welcomed Parliament continuing to push for Ofcom to fully employ all the regulatory powers it was granted under the Act in order to deliver meaningful change. He told us that Ofcom “cannot be deterred” from exercising the regulatory powers it has been given but that “It makes a tremendous difference to [Ofcom] to know that [they] have the continued full-throated support of parliamentarians and Government in doing the job that Parliament has given [them].”²⁶⁷ When we asked the Minister about scrutiny of the implementation process, he argued that Parliament has oversight of Ofcom’s implementation through the Secretary of State, although he did acknowledge that as an independent regulator Ofcom was also directly answerable to Parliament,²⁶⁸ for example through the House of Commons Culture, Media and Sport Committee and Science, Innovation and Technology Committee and the House of Lords Communications and Digital Committee.

198. CONCLUSION

The Online Safety Act 2023 has the potential to deal with many of the issues of online threats to MPs and candidates that we have identified. In particular, it could force platforms to properly resource their content moderation teams, remove illegal content, and grant some oversight of how their content recommendation algorithms function.

199. CONCLUSION

However, whether or not it does so will depend on how it is implemented. For the sake of the affected individuals and democracy as a whole, the abuse targeting MPs and candidates that has become commonplace on platforms must stop, and we are encouraged to hear that Ofcom is focused on this as a measure of success. Phase 3 has the potential to give MPs, candidates, and other users an opportunity to operate free from abuse, which we encourage everyone to seize. However, that opportunity will only materialise if Ofcom makes full use of all the regulatory powers it has been given under the Act.

267 [Q390](#)

268 [Q398](#) For example the House of Commons Culture, Media and Sport Committee and Science, Innovation and Technology Committee have both held inquiries into the Work of Ofcom (Oral evidence taken by the Culture, Media and Sport Committee on 6 May 2025, [Qq 1-92](#); Oral evidence taken by the Science, Innovation and Technology Committee on 20 May 2025, [Qq 1-123](#)) and the House of Lords Communications and Digital Committee holds regular evidence sessions with Ofcom leadership (Oral evidence taken by the House of Lords Communications and Digital Committee on 11 July 2025, [Qq 1-22](#))

200. RECOMMENDATION

In order to ensure that the Act meets the aspirations Parliament had for it once fully implemented, Parliament must continue to have a say in its implementation. The processes for approval for implementation of the Online Safety Act make it challenging for parliamentary committees to scrutinise codes of practice in an effective and timely manner. Whilst two thirds of the Act is now in force, there remains an opportunity for Parliament to engage in the implementation of the third phase and in any future revisions. As the Act comes into force it is also vital that Parliament has the opportunity to assess its effectiveness. Ofcom must make available to Parliament the information to facilitate this scrutiny.

- Ofcom should facilitate scrutiny by keeping the relevant parliamentary committees well-informed of upcoming milestones, including notifying them of consultations, codes being sent to the Secretary of State for approval, and anticipated windows for parliamentary engagement and scrutiny.
- Ofcom must lay a bi-annual report before Parliament, which we encourage the relevant parliamentary select committees to engage with. This report should set out, as a minimum:
 - data and updates on i) compliance and ii) investigative/enforcement action; and
 - Ofcom’s assessment of the Act’s impact on i) platform behaviour and ii) user experience.

Strengthening the Online Safety Act 2023

- 201.** Several witnesses suggested that the Online Safety Act had not gone far enough and would need to be strengthened. We were told that further primary legislation was required to cover “wider forms of toxic communication beyond that which is covered by the Online Safety Act and that which is deemed unacceptable by social media platforms, particularly in view of the sometimes lax and varied definitions of acceptability provided by the platforms in their regulations.”²⁶⁹ Ofcom noted that the Act does not give them powers to tackle “important issues of great concern to people”, although cautioned about expansion, noting that “even the job we have is broad”.²⁷⁰ Talitha Rowland, Director for Security and Online Harms, Department for Science, Innovation and Technology, noted that the constant

269 Dr Diana Maynard (Senior Research Fellow at University of Sheffield); Professor Kalina Bontcheva (Professor at University of Sheffield) ([SCS0014](#)); Alison Giles CB also expressed “a degree of scepticism about whether it will be sufficient” ([Q124](#))

270 [Q385](#) [Mark Bunting]

progress in technology meant that, although the Act was designed to be technology neutral “it will not capture everything, ... and I am sure Ministers will want to look at that.”²⁷¹

- 202.** Particular concerns have been raised that the current regulatory system does not provide sufficient protection against abuse at elections. The Online Safety Act Network argued “Elections and the time around them are foreseeable high-risk periods. The Online Safety Act should be amended to require online platforms to assess and mitigate these foreseeable risks.”²⁷² The Public Administration and Constitutional Affairs Committee has also recommended that “Ofcom in coordination with the Electoral Commission set out the timescale for setting up arrangements to address online abuse and intimidation at elections.”²⁷³ The Online Safety Act Network has proposed that these arrangements should include introducing an elections code of practice, in line with the other codes of practice introduced for social media platforms under the Online Safety Act, to address abuse directed at candidates, elected representatives, campaigners or election officials that could harm the electoral process.²⁷⁴ The network suggested that the Government should use the Bill it intends to bring forward during this Parliament on electoral reform as the legislative vehicle to mandate Ofcom to produce this additional code.²⁷⁵
- 203.** BCS, The Chartered Institute for IT, a professional body for the technology sector, warned that strengthening the Online Safety Act to address “legal but harmful” content could be challenging. They stressed that “If you can’t define it in law, you can’t expect an algorithm to spot it.”²⁷⁶ The Government has indicated that they also believe this “legal but harmful” content is where the challenge of future regulation would fall. Kanishka Narayan MP told us that for illegal content there is now a “clear regulatory system” of platform responsibilities and the regulator’s investigation and enforcement powers, and that any issues were likely to be in how the Act was enforced, while for legal but harmful content “there is a much deeper challenge”, particularly around “the right regulatory balance between free expression and appropriate harm prevention.”²⁷⁷

271 [Q397](#)

272 Online Safety Act Network ([SCS0001](#))

273 Public Administration and Constitutional Affairs Committee, Second Report of Session 2024–26, [Review of the 2024 general election](#), HC487, para 173

274 For a brief explanation of the role and effect of codes of practice under the Online Safety Act see Box 2.

275 Online Safety Act Network, [Delivering Improved Online Safety for Candidates During Elections: A Proposal for a Code of Practice](#), September 2025; DEP2025–0503 ([Restoring trust in our democracy: Our strategy for modern and secure elections](#)) Ministerial Foreword

276 BCS, The Chartered Institute for IT ([SCS0025](#))

277 [Q395](#)

- 204. RECOMMENDATION**
Ofcom must be given time to fully implement the Online Safety Act, in line with the recommendations made above. However, given how central social media is to the issue of threats against MPs and candidates, as well as so many areas of public and private life, it is unlikely that this is the last legislation Government will need to pass on social media regulation. Given the exceptionally complex, technical and politically charged nature of this topic, preparations should be made ahead of time so that options for further regulation are ready for the Government to act on when needed.
- 205. RECOMMENDATION**
These preparations should take account of the fact that political discourse online drives more abuse than other topics and should therefore include consideration of what additional protections platforms may need to put in place around political discussions. These may include prohibiting platforms from having different standards for removing threats against politicians and other public figures, or requiring the introduction of automated prompts like those we called for above, to warn users if they are about to post content that may be abusive, or to encourage them to engage appropriately when contacting an elected representative.
- 206. RECOMMENDATION**
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.
- 207. RECOMMENDATION**
The Government should also note the amount of work required of Ofcom to regulate such a large and evolving sector and prioritise ensuring that it is properly resourced to take on this task.

Disinformation

- 208.** As we noted in our first report, “addressing disinformation is a necessary step for reducing abuse and intimidation against MPs and candidates, as many cases are triggered by disinformation about the victim.”²⁷⁸ We have

²⁷⁸ Speaker’s Conference, First Report of Session 2024–26, [Speaker’s Conference on the security of MPs, candidates and elections](#), HC 570, para 50

heard that it is a particular issue online, with Jessica Zucker telling us that it made up around 40% of the online harms reported in Ofcom’s 2024 Online Nation report, and increased around the election.²⁷⁹

- 209.** One of the most concerning issues we have heard about disinformation online is the use of generative AI to create deepfake pornography targeting female MPs and candidates. We have heard extremely distressing evidence about the scale of this abuse at the last election and the deep hurt it does to the women targeted.²⁸⁰
- 210.** The Online Safety Act introduces a False Communications Offence for online disinformation, which criminalises communications that are known to the sender to be false and sent intending to cause harm. The Government told us that this would mean that social media platforms would be compelled to remove deliberately harmful disinformation when notified.²⁸¹ In 2024 (the year the offence came into force) there were 14 convictions under the false communications offence.²⁸²
- 211.** Some witnesses suggested further legislation was needed to directly tackle disinformation online.²⁸³ Specific suggestions for legislation regarding disinformation about candidates and MPs came from the Electoral Commission who suggested amending section 106 of the Representation of the People Act 1983, which criminalises making false statements about a candidate’s personal character or conduct, to make it clear that the offence covers deepfakes,²⁸⁴ and from Full Fact who suggested adding section 106 offences to the list of priority offences which social media platforms must take active measures to identify and reduce the risk of users encountering on their platforms.²⁸⁵

279 [Q358](#)

280 Glitch ([SCS0018](#)); Electoral Commission ([SCS0020](#)); BCS, The Chartered Institute for IT ([SCS0025](#)); Anonymous ([SCS0044](#)); [Q71](#) [Vijay Rangarajan]; We have also heard other extremely distressing evidence on some of incidents which we have not published to avoid causing further distress to the victims.

281 Home Office ([SCS0042](#)); As we noted above, Ofcom have been clear that for crimes that require a particular intention, platforms do not need to have evidence of the poster’s mental state, and should remove content if they have “reasonable grounds to infer that content is likely to be illegal” ([Q352](#) [Mark Bunting]).

282 Letter from the Parliamentary Under-Secretary of State for Science, Innovation and Technology to the Chair regarding evidence to the Conference on 9 September 2025, [15 September 2025](#)

283 Clean up the Internet ([SCS0007](#)); BCS, The Chartered Institute for IT ([SCS0025](#)) suggested the Government consider strengthening the Act in this way but warned that, unless disinformation could be clearly defined in law, this could prove challenging to enforce.

284 Electoral Commission ([SCS0049](#)); Full Fact ([SCS0056](#)) also supported this proposal

285 Full Fact ([SCS0056](#))

212. However, our first report noted that there were other challenges with the enforcement of section 106, noting that, among other issues, it is rarely prosecuted, challenging to prove and covers only statements about a candidates' personal character not professional conduct. We therefore recommended that the Government "Review how to make the intention behind section 106 of the Representation of the People Act 1983, regarding false statements of fact in relation to a candidate's personal character or conduct, enforceable and able to keep pace with technological developments in AI and deepfakes."²⁸⁶

213. RECOMMENDATION

The Conference's first report noted issues with the enforcement of section 106 of the Representation of the People Act 1983 and recommended the Government review how to make the intention behind it enforceable. False statements of this kind are a particular concern when shared online: we therefore recommend that the Government give appropriate consideration to how any updated legislation can be enforced against online disinformation. As part of this work, and in order to ensure the same issues with enforcement are not repeated, the Government should review the enforcement and effectiveness of the false communications offence introduced by the Online Safety Act 2023. In line with the recommendation in our first report, and in order to address the terrible spread of sexually explicit deepfakes targeting female candidates, the Government should ensure that current legislation and any amended legislation on false statements about candidates explicitly cover the creation of deepfakes.

Additional online offences

214. The Conference sought evidence on whether there needed to be changes to offences that would strengthen the deterrent effect of the criminal justice response to individuals who engage in threatening behaviour or communication. The Crown Prosecution Service (CPS) did not consider there to be "a pressing need for further offences" but they did identify two areas for consideration: doxing (the act of publishing personal information about an individual without their consent); and pile-on harassment (where multiple people collectively target and harass a single person).²⁸⁷

286 Speaker's Conference, First Report of Session 2024–26, [Speaker's Conference on the security of MPs, candidates and elections](#), HC 570, paras 50, 57

287 Crown Prosecution Service ([SCS0024](#))

215. CPS said that whilst there are offences under which such acts could be prosecuted (noting in particular the provisions of section 7(3A) of the Protection from Harassment Act 1997²⁸⁸), there is nothing that specifically addresses these issues and the applicability of existing offences requires complex interpretation. We note that Almudena Lara, Director of Online Safety Policy, Ofcom, told us that Ofcom is currently consulting on “the pile-ons and harassment that women suffer, especially women in high-profile and political roles” and would set “clear expectations for services on foundational steps that we expect them to take as well as good practice that we expect them to address.”²⁸⁹

216. When asked whether the Government had given consideration to introducing new legislation to address doxing and pile-on harassment, Kanishkya Narayan MP told us “we are working across departments with shared interest in this cross-cutting issue to carefully consider the points made by the CPS and potential options in response”.²⁹⁰

217. RECOMMENDATION

Doxing and pile-on harassment cause significant distress but are not sufficiently addressed by existing legislation. The Government should introduce legislation that is specifically designed to address these issues at the earliest opportunity.

288 Section 7(3A) makes anyone who has “aided, abetted, counselled or procured” someone to act a certain way, or say a certain thing, responsible for that conduct as if it were their own (as well as the person who acted).

289 [Q358](#)

290 Letter from the Parliamentary Under-Secretary of State for Science, Innovation and Technology to the Chair regarding evidence to the Conference on 9 September 2025, [15 September 2025](#)

4 Conclusion

- 218.** Our first report sought to understand the threat level against MPs, candidates and elections, and the effectiveness of the response to it. We identified solutions in areas where the security of individuals and electoral processes could be strengthened. But ultimately, we concluded that whilst physical security provision must be responsive to the changing threat landscape, such measures have gone as far as is currently deliverable and practical. Politicians want to be accessible to their constituents and connected to their communities. Further physical security measures would result in a fundamental and undesirable change in their ability to carry out their role in this way.
- 219.** Yet evidence confirmed what we knew to be true anecdotally through our own experiences or conversations with our colleagues; recent years have seen a significant change in the level and nature of threats against MPs and candidates, creating a toxicity in political discourse that affects politicians' sense of safety and has a corrosive effect on democracy.
- 220.** When vulnerability reduction measures are maximised, the only way to increase MPs' and candidates' sense of safety is to reduce the threats they face. This has been the focus of our second phase of work.
- 221.** This report has considered the public attitudes leading people to engage with political representatives in an abusive and aggressive manner. We have never questioned the importance of passionate debate, disagreement and discourse, which are central to any healthy democracy. But too often, a line is crossed, sometimes resulting in a criminal act, but most of the time leading to comments and behaviours that whilst not criminal, are harmful to the individual and democracy as a whole, because they reduce the willingness of people, particularly those in underrepresented groups, to stand for office. We hope that our recommendations on citizenship education in schools and a wider public awareness campaign will help people to understand where that line is. People's understanding of what is appropriate would also be improved by more measured campaigning by political parties and others. We are confident that, as recommended in our first report, the Speaker will be able to work with the political parties represented in Parliament, and the Electoral Commission, to define a collectively agreed set of principles to guide behaviours and language when campaigning. This work will start in earnest in 2026, and we once again urge all relevant parties to engage constructively in the process.

- 222.** We know that it is only a minority of people who actively abuse politicians. But the impact of the actions of a few is substantive. Society must demonstrate to them that it does not condone their activities and raise the social cost of engaging in them. Where abuse is legal but harmful we hope this message can be conveyed through education and better political literacy. Where it crosses the line into criminal behaviour, we have made recommendations for more robust and consistent policing, prosecutorial decisions and sentencing outcomes which will reflect the serious impact these crimes have on democracy.
- 223.** Our survey found that the vast majority of abuse experienced by MPs occurs online, particularly on Facebook and X. The small steps Meta and X have taken to equip users with tools to shield themselves for abuse do little to tackle the root of the issue. That will require larger, fundamental change in the way the platforms moderate and promote content. We have no faith in social media companies taking such steps voluntarily.
- 224.** The Online Safety Act 2023 is the first step in what we anticipate will be a long and ongoing journey of social media regulation. Ofcom must be bold in its implementation and rigorous in its enforcement of the Act. But already, challenges exist beyond what the Act sought to address, such as those presented by disinformation, generative AI and deepfakes, and doxing and pile-on harassment. Government must also therefore be on the front foot in considering what further legislation is required, not least because the pace at which technology evolves is far greater than that with which governments can legislate.
- 225. CONCLUSION**
Our reports have highlighted that tackling threats against MPs, candidates and elections will require a focused, co-ordinated effort across multiple organisations. We hope that the recommendations made in our two reports help shape an agenda for change that improves the current climate of abuse and intimidation affecting the daily lives of MPs, their staff and families, which causes significant harm to democracy.

Annex 1: Conclusions and Recommendation from the First Report of the Speaker's Conference on the security of MPs, candidates and elections (HC 570)

Threats against candidates and MPs and their impact on the democratic process

1. To be elected as a Member of Parliament is an honour and privilege, and it is one of the most important and rewarding jobs any of us have undertaken. Robust political discourse and challenge is an important part of the role that we want to protect and encourage. (Conclusion, Paragraph 13)
2. However, the current level of threats against MPs and candidates is stifling debate and weakening democracy as a whole. It is dissuading candidates from standing and making it harder for MPs and candidates to engage with the public. It is improperly influencing political decisions by forcing people to weigh the public good against their own safety and the wellbeing of their colleagues, their staff and their families. Because of the threat of abuse, some MPs already self-censor by not speaking about contentious issues, and on rare occasions it can even affect their voting intention. Abuse and intimidation are not part of the job of being an MP and threaten the health of our democracy. (Conclusion, Paragraph 14)
3. Politicians have a responsibility to their constituents and must be accountable to their electorates for their decisions. It is to be expected that some constituents will disagree with decisions a politician has made. Everyone has a right to try to influence their MP's positions and ultimately hold them to account at the ballot box. However, personal abuse and threats to the safety of MPs because of how they have spoken or voted are never appropriate. Yet increasingly people think it is acceptable to engage

with politicians in a confrontational, aggressive manner. Some people even believe that MPs and candidates should expect some level of abuse as part of the job: a view we wholeheartedly reject. We will consider the public attitudes that drive this behaviour, and the ways such societal tendencies can be halted and reversed in our second phase of work. (Conclusion, Paragraph 18)

4. The nature and tone of engagement on, as well as policies and approaches of some social media platforms, are contributing to the level of threats against MPs and candidates. Although many MPs and candidates choose to ignore insults and allegations online, either because of a mistaken belief that they are to be expected or because of the difficulties and expense of trying to have them removed, libelous smears or hyperbolic attacks are sometimes taken literally and can lead people who believe them to aggressively confront the MP or candidate in real life. We will return to the role of social media in our second phase of work. (Conclusion, Paragraph 20)
5. While we respect and wish to protect the right of the press to hold politicians to account fairly and honestly, how the press report on politicians and Parliament shapes public attitudes towards MPs and candidates and can add fuel to the fire, which is at best unhelpful, at worst, causes real harm. We will return to this issue in our second phase of work. (Conclusion, Paragraph 22)
6. We are acutely aware that the way politicians engage with each other shapes people's perception of how politics is done. MPs and candidates have a responsibility to lead by example and we must all strive for courtesy and respect in our politics. (Conclusion, Paragraph 27)
7. There should be a code of conduct for all candidates, MPs and parties that defines a collectively agreed set of principles to guide behaviours and language when campaigning. The Speaker will work with the parties currently represented in Parliament and the Electoral Commission to develop such a code, in order to ensure it meets the needs of the broad range of candidates who stand in elections. Not wanting to preclude the uptake of this code of conduct for other elections, the Speaker will also invite representations from the Local Government Association as part of this process. (Conclusion, Paragraph 28)
8. The leadership of all parties represented in Parliament and the Electoral Commission should engage constructively with the Speaker to develop a code of conduct for campaigning, to be agreed and in place at the next general election. (Recommendation, Paragraph 28)
9. Parties have a duty of care to their candidates, particularly during election periods. (Conclusion, Paragraph 29)

10. They should ensure all candidates and agents are aware of how to report threats to, or request support from, appropriate external agencies. Parties should also offer candidates and agents appropriate avenues within the party for raising issues they may be having with abuse and intimidation, so that they are aware of the scale of threats against their candidates. The precise mechanism for gathering this information will vary according to party size and resources and should not compel or pressure candidates to share cases or details they do not wish to. (Recommendation, Paragraph 29)
11. Parties also have a responsibility to properly vet and select candidates who would be appropriate MPs, in line with legal restrictions on who can stand for election. We will return to the question of whether current legal restrictions on standing for election are sufficient in our second phase of work. (Conclusion, Paragraph 30)

Effectiveness of the response: Elections

12. At the dissolution of Parliament for an election, all MPs wishing to continue in the role become candidates and the Parliamentary Security Department (PSD) ceases to have responsibility for their security. But security risks and concerns remain. Overall, the arrangements made between the Home Office and PSD for the 2024 General Election, as well as other security provisions introduced through the Defending Democracy Policing Protocol, were welcome and effective. (Conclusion, Paragraph 35)
13. The immediate transfer of the capacity to provide candidates with private security operatives from PSD to the Home Office should be established as a default arrangement for future general elections, effective from the moment of dissolution. (Recommendation, Paragraph 36)
14. The Government should monitor and record the use of Disqualification Orders under the Elections Act 2022, review their effectiveness, and report the results to Parliament by means of a Written Ministerial Statement. The Government should also submit a report to the Speaker's Committee on the Electoral Commission, as soon as feasibly possible and at the latest in time for reforms to be implemented at least six months before the next general election, in line with the Gould principle. (Recommendation, Paragraph 37)
15. Elections occur infrequently and present policing challenges that exist alongside every police force's "business as usual". We recognise this strain and thank the police for their work, during the election and every day since. Policing elections is hard. Electoral law is complicated and disparate. The negative trends described in this report have changed what it means to police elections. The focus has moved from matters of fraud and other administrative malpractices, to dealing with incidents of alleged political

abuse and intimidation. The current structures for policing elections fail to reflect this shift. We will return to these structural issues in our second phase of work. (Conclusion, Paragraph 43)

16. The policing response during the 2024 general election period was mixed, in terms of the level of engagement police had with candidates, their presence at hustings, polls and counts, and the handling of incidents. The issue of inconsistency in police responses to incidents of abuse and intimidation is a significant challenge, which we cover elsewhere in this report. Engagement and resourcing during an election period can and must be planned for through comprehensive, risk-assessed policing plans. (Conclusion, Paragraph 44)
17. Every police force should produce a fully risk-assessed policing plan ahead of a general election period. As a minimum, such plans must:
 - identify potential “flashpoint” events and ensure an appropriate police presence is available for them; and
 - account for the potentially higher risk profile some candidates may have, either carried over from their time as an MP, because of their own prominence, or for other factors affecting their level of risk, whilst ensuring no political advantage is given to any candidate.

The national portfolio lead for policing elections should take steps to ensure this is done in a consistent and standardised way, with input from local returning officers and processes for keeping the plan under review throughout the election period. Candidates and relevant parties should be able to contribute to plans if they wish to do so. Similar plans should be drawn up and implemented for by-elections if they occur. (Recommendation, Paragraph 45)

18. Government guidance and advice on security for candidates in the 2024 General Election was welcome, but its reach was limited in part because of a lack of understanding of data sharing powers by returning officers. (Conclusion, Paragraph 48)
19. The Government and the Electoral Commission should investigate reforms to the system for candidate registration so that candidates and agents are asked to provide an email address at registration which can be shared with the Electoral Commission and the police. This will allow the Electoral Commission and the police to send security guidance directly to all candidates. While these reforms are being considered and implemented, the Electoral Commission should provide guidance to returning officers to signpost every candidate to the single source hosting security-related guidance and advice, as well as relevant local security information, at the point they register. (Recommendation, Paragraph 48)

- 20.** When it comes to tackling harassment, abuse and intimidation of candidates, electoral law is not fit for purpose. Whilst there are specific offences designed to deal with these issues, they often lack clarity, are outdated, or do not reflect challenges of the modern context. Because of one or all of these factors, the existing offences are little used and ineffective. (Conclusion, Paragraph 56)
- 21.** The Electoral Commission should produce a code of practice for election officials, drawing together all the necessary information related to the safety and security of candidates. (Recommendation, Paragraph 56)
- 22.** The Government must undertake a full review of electoral law with the intention of identifying:
 - offences that require clarification through legislative change or further guidance;
 - gaps in the powers of returning officers to ensure the effective administration of elections in the context of situations relating to harassment, abuse and intimidation; and
 - administrative practices or processes that unintentionally undermine security or electoral integrity.

As a minimum, the Conference recommends that the Government:

- a.** Remove the option for any home addresses to be published as part of the nomination process. Instead, UK parliamentary election ballots should state which constituency each candidate lives in.
- b.** Introduce ID and address checks for all candidates.
- c.** Work with the Electoral Commission to review the adequacy of nomination requirements in protecting elections from candidates seeking to mislead the electorate or undermine the integrity of the democratic process.
- d.** Clarify what behaviour is and is not permissible outside a polling station.
- e.** Introduce a new power for returning officers to work in collaboration with the police to extend the protective perimeter around a polling station in certain circumstances.
- f.** Update, or clarify the scope of, the offence of causing disturbances at election meetings under section 97 of the Representation of the People Act 1983.

- g.** Review how to make the intention behind section 106 of the Representation of the People Act 1983, regarding false statements of fact in relation to a candidate's personal character or conduct, enforceable and able to keep pace with technological developments in AI and deepfakes. This should include consideration of expanding the offence beyond personal character and conduct, and the challenges of disproving the statutory defence of honest belief.
- h.** Update, or clarify the scope of, the provisions of paragraph 42 of Schedule 1 to the Representation of the People Act 1983 to more clearly identify the circumstances in which the presiding officer can adjourn a poll.

Whilst our remit is for parliamentary candidates and elections, we encourage Government and the devolved Administrations to ensure that, where possible and appropriate, a consistent approach is taken across all elections. (Recommendation, Paragraph 57)

Effectiveness of the response: security of MPs

- 23.** Security measures for MPs have come a very long way in recent years, but the political environment has also changed dramatically. It is not for the Speaker's Conference to assess the safety of individual MPs. Rather, we will focus on the effectiveness of measures at making MPs feel safe within the context of the threats most visible to them. (Conclusion, Paragraph 61)
- 24.** Despite the step change in vulnerability reduction measures over recent years, many MPs remain concerned for their safety, as well as that of their staff and families. However, we agree with the assessment that a further step change in vulnerability reduction measures is not currently deliverable and would lead to a fundamental and undesirable change in the way MPs carry out their roles and engage with their constituents. Improvements need to come from encouraging appropriate uptake and effective delivery of existing measures, since issues with the delivery of security measures undermine MPs' confidence in the service itself. In turn, this diminishes their sense of safety which can affect their willingness to continue to serve in public office. Above all, the focus must be on reducing the level of threat posed to MPs and candidates. Threat reduction will be at the centre of our second phase of work. (Conclusion, Paragraph 67)
- 25.** Notwithstanding our conclusion against a further step change in security arrangements, what is being done can always be done better. PSD's work relating to families and its focus on online safety are necessary and welcome. But the political landscape in which MPs operate is continually changing and recent experience demonstrates how global events can drive

domestic discourse and action. Both can have implications for the security of MPs and any future reforms must anticipate, rather than respond to the risk. (Conclusion, Paragraph 69)

- 26.** PSD should continue to be proactive and flexible in assessing how significant events or trends might change the security needs of MPs and should be prepared to adapt its security posture in anticipation of any changes in the threat landscape. PSD's security arrangements for individual MPs must continue to respond to their professional assessment of anticipated risk. In exceptional circumstances where the level of abuse and intimidation against an MP means there is also an identified threat to their staff, PSD should consider flexible and pragmatic arrangements to ensure appropriate security for those staff. (Recommendation, Paragraph 69)
- 27.** MPs have a vital role to play in their own security. They must take it seriously and engage with PSD, not only for themselves but as a duty of care towards their staff. (Recommendation, Paragraph 70)
- 28.** As part of their duty of care as employers, MPs must ensure their staff are aware of the security offering available to them and take their views into account when considering their own security, particularly in relation to the installation of security measures in constituency offices and the use of security operatives during surgeries. (Recommendation, Paragraph 71)
- 29.** A consistent, swift response to reported incidents of abuse and intimidation is integral to MPs' sense of safety and their ability to effectively carry out their role. But consistency does not currently exist, either between or within police forces, or across the criminal justice system. Inconsistency weakens the deterrent effect and empowers perpetrators. In our second phase of work we will undertake an end-to-end review of the criminal justice response to crimes that undermine democracy and identify recommendations for how it could be strengthened. Specifically, we will explore the merits of a more centralised approach to policing these issues, noting the need to consider the different policing and legal systems across the UK. (Conclusion, Paragraph 79)
- 30.** Some change need not wait. The Government should ensure that all parts of the criminal justice system drive a cultural shift and ensure relentless challenge of the perception that abuse and intimidation comes with the job of being an MP. Its response to this report should list the steps it intends to take to achieve this. (Recommendation, Paragraph 80)
- 31.** There is at best inconsistent understanding and awareness amongst police officers of relevant electoral, communications and public order offences as they relate to electoral events or politicians. Even when offences are widely known, several lack clarity on the criminal threshold. This places undue

pressure on the judgment of the responding officer, who may be operating in a politically charged and sensitive environment, in considering whether an offence may or may not have been committed. (Conclusion, Paragraph 86)

32. The police, Crown Prosecution Service and Government should work together to develop guidance that clarifies the criminal thresholds for communications, electoral and public order offences as they relate to incidents of abuse and intimidation of MPs and candidates, or electoral events. This guidance must form the basis of training for returning officers and police officers. MPs and candidates should also have access to this guidance, so they are better informed on what and when to report issues and the response to expect. Equivalent guidance with input from the relevant bodies should be developed in the devolved nations. (Recommendation, Paragraph 87)
33. Whilst most incidents of abuse or intimidation experienced by MPs and candidates do not meet a criminal threshold, the distinction is often irrelevant in terms of the impact they have. Repeated “low level” abuse and intimidation is wearing on the individual and corrosive to our democracy. (Conclusion, Paragraph 91)
34. The police must adopt a preventative, proactive approach to policing harassment, abuse and intimidation against MPs. PLaiT must renew its focus on offender management, and work with the Bridger Network and Chief Constables to develop guidance on interventions for non-criminal incidents, including the use of anti-social behaviour legislation. Police Scotland and the Police Service of Northern Ireland should consider what similar legislative tools are available to them to facilitate an equivalent response to non-criminal incidents. (Recommendation, Paragraph 91)
35. Neither MPs nor their staff should assume responsibility for determining what does and does not warrant reporting. MPs and their staff must report to the police any incident that strikes them as abusive or intimidatory. (Recommendation, Paragraph 92)
36. Local police forces and PLaiT must ensure that MPs, candidates or their staff, are kept informed of action taken, progress of investigations and outcomes of reported incidents. In line with the Victims’ Code, the police should ask and establish how often an MP or candidate wishes to receive updates on their case and keep them informed in line with those preferences. (Recommendation, Paragraph 94)
37. As part of our second phase assessment of the criminal justice system’s response to crimes that undermine democracy, we will explore in greater depth the adequacy of the existing legislative frameworks and criminal justice processes giving particular consideration to: the merits or otherwise of a) a specific offence against MPs and b) an aggravating factor applicable

to sentencing for crimes committed against candidates or MPs because of their role; and whether the classification of threats of violence against MPs under existing offences appropriately reflects their seriousness in the context of their impact on democracy. (Conclusion, Paragraph 97)

The Conference's next phase of work

38. Given the limits of vulnerability reduction, more work must be put into understanding what is driving the threat level, and how it can be reduced. This will be the focus of the next phase of our inquiry. We have identified three areas where we believe we may be able to make practical recommendations that could reduce the level of threats against candidates and MPs:

- Public attitudes towards MPs and the level of abuse and intimidation in political debate, including the influence of the press and broadcast media.
- How threats against MPs and candidates are handled in the criminal justice system.
- The role of social media in promoting or combatting threats against MPs and candidates. (Conclusion, Paragraph 99)

Annex 2: Speaker's Conference submission to the Editors' Code of Practise Committee

About the Speaker's Conference

On 14 October 2024, the House of Commons passed a Motion to establish a Speaker's Conference. The Conference, which operates as a cross-party committee of MPs, was directed by the House to: "consider the factors influencing the threat levels against candidates and MPs and the effectiveness of the response to such threats; and make recommendations about the arrangements necessary to secure free and fair elections and the appropriate protection of candidates at future UK-wide parliamentary elections and of elected representatives thereafter".

The Conference published its first report in June 2025. That report concluded that "how the press report on politicians and Parliament shapes public attitudes towards MPs and candidates and can add fuel to the fire, which is at best unhelpful, at worst, causes real harm." The Conference committed to further examine this issue in its second phase of work and its findings were included in its final report, published in October 2025.

This submission is the result of the conclusions of that report, recommending change to the Editor's Code of Practice as it relates to headlines, doorstep and approaches to families. The Conference's evidence and recommendations are summarised below.

The role of the press

Headlines

Whilst Clause 1(i) of the code specifies that headlines must be accurate, evidence to the Conference's inquiry suggested that it is often assumed that headlines will be read in the context of the article. However, some

research suggests that the majority of people only read headlines, which are often oversimplified or present a perspective that is caveated, or even contradicted by, the article below. The Conference therefore concluded:

In a click-bait, fast-read culture, headlines have a key role to play. However, where headlines are disproportionately negative, read without reference to the full article, or trigger unjustified hostility towards their subjects - be they MPs and candidates or other public figures - that can lead to abuse.

The Conference recommends that:

IPSO should amend its press regulation code to specify that a story's headline should be accurate, and clearly distinguish between comments, conjectures, allegations and facts, when read on its own, in line with the current Impress code.

Doorstepping

Clause 3 of the Code of Practice requires that journalists do not engage in intimidation or harassment when covering a story, but this is subject to the public interest exemption. Whilst practice has come a long way, we have heard much evidence, both formally and anecdotally, that MPs, candidates and other public figures continue to be subject to aggressive and invasive methods to investigate news stories. Of most serious concern is intimidatory behaviour that occurs at their home. This practice of “doorstepping” affects families, including children, and is particularly intimidatory.

Witnesses to our inquiry, Anushka Asthana, Deputy Political Editor at ITV News and Chair of the Parliamentary Press Gallery, and David Hughes, Political Editor at PA and Chair of the Parliamentary Lobby, argued that this approach is justified when someone has refused to comment via other means and journalists wish to demonstrate to their audiences the efforts made to get an answer.

The Speaker's Conference rejects this argument, concluding:

The press's practice of doorstepping MPs and candidates at their homes intimidates them and their families and undermines their sense of safety. It normally produces nothing except a video or a photograph of the person waving away cameras from their house, which adds no information to justify a public interest defence. If anything, the practice of doorstepping when people decline to comment operates as an implicit threat: "Give us a quote, or we'll come to your house."

The practice of doorstepping has evolved over time, but needs to evolve further. In future, if the press truly believe they need to show proof that they have made appropriate efforts to contact someone, any doorstepping should occur at their known place of work, or in another professional setting, where they are expected to be.

The Conference therefore recommends that:

IPSO, Impress and Ofcom should amend their press regulation codes to make clear that doorstepping at a residential address is a form of harassment for which there is no public interest exemption. Doorstepping MPs or other official figures should only be acceptable around their offices and other professional settings.

Families

The Conference has also been made aware of, and is deeply concerned by, incidents in which journalists have approached MPs' children in an attempt to mislead them into revealing information about their parents. Whilst evidence to the Conference confirmed that the press should not approach family as part of covering a story, it is clear to us that the provisions in place that are intended to prevent this practice are not working and must be more clearly stated.

The Conference therefore recommends that:

IPSO, Impress and Ofcom should amend their press regulation codes to make clear that children, spouses or other family members should not be used as a way of gaining access to or information on an MP, or any other public figure. There should be no public interest exemption for this conduct.

The Conference welcomes the Committee's consideration of these proposals and would be happy to discuss them further.

Annex 3: Draft statutory aggravating factor (hostility to the democratic process)

To move the following Clause—

“Aggravating factor: hostility to the democratic process

In the Sentencing Act 2020, after section 66 insert—

“66A Hostility to the democratic process

- 1.** This section applies where a court is considering the seriousness of an offence committed against a relevant person which is aggravated by hostility to the democratic process.
- 2.** In this section, a “relevant person” means an elected representative, an electoral candidate or a related person (see section 66B which provides further definitions).
- 3.** The court—
 - a.** must treat the fact that the offence is aggravated by hostility to the democratic process as an aggravating factor, and
 - b.** must state in open court that the offence is so aggravated.
- 3.** For the purposes of this section, an offence is aggravated by hostility to the democratic process if the commission of the offence was motivated (wholly or partly) by an intention to—
 - a.** interfere with the conduct of an election held in England;
 - b.** intimidate the relevant person in the exercise of their functions;
 - c.** inhibit or deter the expression of a political opinion by the relevant person;
 - d.** discourage the relevant person, or any person sharing personal characteristics similar to the relevant person, from participating in politics.

5. For the purposes of subsection (4), it is immaterial whether or not the offender’s hostility is also based, to any extent, on any other factor not mentioned in that subsection.

66B Meaning of “elected representative”, “electoral candidate” and “related person”

1. In section 66A and this section, “elected representative” means—
 - a. a member of the House of Commons;
 - b. a member of a local authority in England;
 - c. an elected mayor in England (within the meaning of Part 1A or 2 of the Local Government Act 2000);
 - d. a mayor for the area of a combined authority in England established under section 103 of the Local Democracy, Economic Development and Construction Act 2009;
 - e. a mayor for the area of a combined county authority in England established under section 9(1) of the Levelling-up and Regeneration Act 2023;
 - f. the Mayor of London;
 - g. a member of the London Assembly;
 - h. a police and crime commissioner in England.
2. In subsection (1)(b), “local authority” means a county council, a district council, a parish council, a London borough council or the Council of the Isles of Scilly.
3. In section 66A and this section, “electoral candidate” means a candidate or future candidate at an election to become an elected representative.
4. In section 66A, “related person” means—
 - a. a person falling within section 34 of the Elections Act 2022 (campaigners);
 - b. a person employed or engaged by an elected representative or electoral candidate for the purposes of assisting the representative or candidate with the exercise of their functions;
 - c. a returning officer or any person exercising, or assisting with the exercise of, the functions of a returning officer under the Representation of the People Act 1983 (see sections 24 and 28).”

Conclusions and recommendations

Public attitudes

1. Most people continue to regard threats against MPs and candidates as unacceptable, and only a small minority of people resort to them. However, this minority is sufficient to lead to most MPs and candidates receiving a persistent stream of corrosive, low-level abuse, along with occasional, highly intimidating spikes in abuse when public attention negatively targets particular MPs and candidates. Like all bullies, the perpetrators often focus on people's personal characteristics, especially anything that is distinctive about them, meaning that women and people from ethnic minority backgrounds generally receive more abuse. (Conclusion, Paragraph 18)
2. It is not clear why this small group choose to abuse politicians and other public figures in this way. But in recent years they have been emboldened by a perception that the behaviour is becoming more acceptable and a widespread erosion of trust in political institutions that is partly a reaction to real failings, but partly the result of a lack of understanding about the political process and the complexity of political decision making, which has let people assume that any political disagreements are due to bad faith motives on the other side. We are also concerned that this group do not appear to be deterred from this behaviour by the existing regulatory and legal framework, and appear to believe they can abuse politicians and public figures with impunity. We return to the effectiveness of the criminal justice system in deterring abuse in Chapter Two. (Conclusion, Paragraph 19)
3. We are aware that there are active debates about freedom of speech and political discourse. These debates are focused on how people can express their views about political questions. These debates do not relate to our work, which is about how people directly treat individual MPs and candidates. Some of the comments MPs and candidates receive may be legitimate disagreements expressed in a rude or uncivil tone, either due to heightened emotion or a lack of awareness of how they will be received. We are deeply aware of the impact that the decisions politicians make have on people's lives and wellbeing, and understand that people may often feel upset or troubled about a political outcome, or frustrated or dissatisfied with the political system. However, this never justifies deliberate abuse

and threats against individual candidates or MPs. Even if an uncivil or abusive comment is not intended to intimidate, it can still undermine the willingness of the recipient and affected bystanders on all sides to engage in the political process, as well as the argument it is meant to support. We therefore continue to urge everyone to engage positively in the political process, to maintain a courteous and respectful tone in discussions, and to extend grace and understanding to those with whom they disagree. (Conclusion, Paragraph 20)

4. Strengthening citizenship education must form part of any strategy to tackle abuse, harassment and intimidation of politicians. This should begin with a comprehensive programme of citizenship education delivered by trained teachers. (Conclusion, Paragraph 29)
5. The Department for Education's Curriculum and Assessment Review should ensure that the National Curriculum includes a comprehensive programme of citizenship education from KS1 to post-16. Citizenship education needs to start in earnest in primary schools, so that healthy attitudes towards democratic structures and processes are embedded early on. This programme should develop:
 - a. knowledge and understanding of key concepts such as democracy, human rights, the rule of law, media and information literacy, and the different roles and powers of MPs, local councillors, and other elected representatives;
 - b. competencies, particularly in critical and analytical thinking, which are often emphasised in respect of the needs of the economy, but rarely in respect of the needs of democracy, as well as confidence and motivation to actively participate in the democratic process;
 - c. practical experience of deliberating, debating, and applying concepts in real-world scenarios to learn the trade-offs involved in policy formation;
 - d. an awareness of how the tone of discussions, particularly uncivil or rude language, affects others participating in or observing the debate, and how abuse and intimidating behaviour towards politicians affects democracy, along with an understanding that abusive behaviour comes from only a small minority of people;
 - e. an understanding of the responsibilities citizens have to maintain a healthy democracy, including around voting and participating in the democratic process.

Teachers must receive appropriate training to deliver citizenship education confidently and impartially, and it must be implemented as an integral part of any proposals to lower the voting age to 16.

We invite the devolved Administrations to consider what, if any, changes can be made to citizenship education in the Welsh, Scottish and Northern Irish curricula to ensure they also deliver the knowledge, skills and understanding outlined above. (Recommendation, Paragraph 30)

6. MPs should actively engage with young people in their local areas to support citizenship education. To help them to do this effectively, Parliament's Education and Engagement Team should expand its offer to MPs to include resources for presentations and practical workshops that are designed by educators with expertise in working with different age-ranges. Parliament's Education and Engagement Team should also extend the training and guidance on working with children that is currently offered to Members of the House of Lords to any MPs who want to take part. The House of Commons should make available the resources to cover this expansion, based on an assessment of anticipated uptake among MPs. (Recommendation, Paragraph 33)
7. We encourage MPs to engage with students in their constituency. UK Parliament Week presents a good opportunity for them to visit schools. The Education and Engagement Team should help to facilitate these visits, working with MPs and managing the administrative tasks to enable them to meet as many students as possible. (Recommendation, Paragraph 34)
8. Although the scope of our work covers only MPs and general election candidates, we encourage local councillors and other elected officials to try to engage with schools in their local area in the same way, and for the relevant local government bodies to similarly support them in doing so. (Recommendation, Paragraph 35)
9. In-school education has the potential to drive a change in the attitudes and behaviour of future voters, but it does not address the abuse of MPs and candidates today. For that, a wider engagement campaign is needed. (Conclusion, Paragraph 39)
10. To reach and change the behaviour of people who are willing to abuse or intimidate MPs and candidates it is essential that any such campaign is based on knowledge of the people involved, their motivations, and the most effective and credible ways to engage with them: whilst the scale and impact of abuse is well-researched and understood, these matters are not. We have tried to answer the questions of why people are abusing politicians and how to change this behaviour. But in the absence of comprehensive research to draw on, the evidence base is insufficient to design a campaign that we could be confident would effectively deliver the change that is needed. (Conclusion, Paragraph 43)

11. We therefore recommend that the Government's Defending Democracy Taskforce commission research to understand the identities and motivations of perpetrators of abuse and intimidation of MPs and candidates (from those engaging in repetitive 'low level' abusive behaviours and communications to those committing criminal offences), and the most effective ways to engage with them and deter them from this behaviour. It should consider the role played by online disinhibition in driving abuse and how to address the disparity in what is considered acceptable behaviour on- and offline, as well as the evidence that exists on the value of working with potential antagonists to spread the message, and the importance of humanising MPs and candidates to people who might abuse them. The findings of this research should inform an engagement strategy that seeks to strengthen understanding of the role of politicians, rebuild trust in political institutions, and highlight the corrosive impact of harassment, abuse and intimidation on democracy. The findings of the research should also be shared with the police to inform offender management strategies. (Recommendation, Paragraph 44)
12. Developing a targeted campaign will take time. In the interim, work should begin to end the perception that abuse of public figures is acceptable. The Defending Democracy Taskforce should run a public health-style messaging campaign using the full range of legacy and new media channels, and drawing on up to date behavioural change techniques and research, to counter the perception that it is acceptable to abuse politicians. The campaign should make clear that the majority of people still regard threats against politicians as unacceptable, to raise the social pressure on potential perpetrators, and that criminal threats are likely to receive a more serious response from the criminal justice system. Noting that abuse is often driven by frustration and a lack of political literacy, it should inform people of the methods for engaging with MPs, candidates and the broader political process and help them understand how to use these effectively and positively. This campaign should consider using non-traditional spokespeople who are likely to encourage engagement from the target audience. (Recommendation, Paragraph 45)
13. As the Fourth Estate, a free press is a core pillar of democracy. It ensures transparency, holds power to account and encourages informed citizen participation. However, just as MPs and candidates have a responsibility to safeguard democracy through their conduct, so too does the media in its reporting. IPSO, Impress and Ofcom must rigorously enforce their codes of conduct and publishers must ensure all journalists they work with, including freelancers, citizen journalists and others they commission or obtain stories from, are clear on their obligations to adhere to those codes. (Conclusion, Paragraph 49)

14. There is no question that factual, fair reporting on matters of public interest and robust debate and disagreement in the public eye are vital parts of any healthy democracy. We agree that the media is not responsible for how the public reacts to those stories. But all too often news stories result in abusive and intimidating commentary; no matter what stories there are about someone in the press, it is never appropriate to threaten them personally. When mistakes are made by people in public office they should be held to account through appropriate democratic and legal means, not by intimidation. (Conclusion, Paragraph 52)
15. Oversimplification or misrepresentation of a story can serve as a catalyst for abuse and create an unnecessary risk to individuals, for which the press must take responsibility and act to mitigate. To address this, we encourage politicians and the press to participate more in long-form interviews and coverage, particularly when considering complex matters. (Conclusion, Paragraph 55)
16. In a click-bait, fast-read culture, headlines have a key role to play. However, where headlines are disproportionately negative, read without reference to the full article, or trigger unjustified hostility towards their subjects - be they MPs and candidates or other public figures - that can lead to abuse. IPSO should amend its press regulation code to specify that a story's headline should be accurate, and clearly distinguish between comments, conjectures, allegations and facts, when read on its own, in line with the current Impress code. The IPSO Editors' Code of Practice Committee's next review of the Code is expected in 2026: the Conference will submit a formal proposal for this change to this review (see Annex 2 for the text of the submission). (Conclusion, Paragraph 59)
17. The press's practice of doorstepping MPs and candidates at their homes intimidates them and their families and undermines their sense of safety. It normally produces nothing except a video or a photograph of the person waving away cameras from their house, which adds no information to justify a public interest defence. If anything, the practice of doorstepping when people decline to comment operates as an implicit threat: "Give us a quote, or we'll come to your house." (Conclusion, Paragraph 69)
18. The practice of doorstepping has evolved over time, but needs to evolve further. In future, if the press truly believe they need to show proof that they have made appropriate efforts to contact someone, any doorstepping should occur at their known place of work, or in another professional setting where they are expected to be. (Conclusion, Paragraph 70)
19. IPSO, Impress and Ofcom should amend their press regulation codes to make clear that doorstepping at a residential address is a form of harassment for which there is no public interest exemption. Doorstepping MPs or other official figures should only be acceptable around their offices

and other professional settings. The Conference will include this proposal in its submission to the IPSO Editors' Code of Practice Committee's next review of the Code (Annex 2). Similar changes should be reflected by Ofcom and Impress in their respective codes when they are next reviewed. (Recommendation, Paragraph 71)

20. IPSO, Impress and Ofcom should amend their press regulation codes to make clear that children, spouses or other family members should not be used as a way of gaining access to or information on an MP, or any other public figure. There should be no public interest exemption for this conduct. The Conference will include this proposal in its submission to the IPSO Editors' Code of Practice Committee's next review of the Code (Annex 2). Similar changes should be reflected by Ofcom and Impress in their respective codes when they are next reviewed. (Recommendation, Paragraph 75)

The Criminal Justice Response

21. Following the concerns identified in our first report that an inconsistent policing response to threats against MPs and candidates reduces their sense of safety and weakens the deterrent effect for perpetrators, it is now clear that a national specialist team approach to anti-democratic crimes, led by a senior body like the National Police Chiefs' Council, would improve the consistency of the police response. The relatively small number of MPs and infrequency of electoral events means that crimes targeting them are too rare for all officers to develop the necessary knowledge and understanding—particularly of the political dimensions and impact such incidents have on democracy—to ensure a consistent and appropriate response. This approach would allow a smaller group of officers to develop expertise to support these investigations. (Conclusion, Paragraph 86)
22. A central capability with specialist officers provides other benefits. There are opportunities to improve intelligence and better manage offenders before threats escalate, by combining the policing of threats against MPs and candidates with the policing of threats against other elected officials and candidates. There is also an opportunity to include the specialist policing of other anti-democratic crimes, such as the dedicated hotline for reporting crimes directed by foreign states that has been recommended by the Joint Committee on Human Rights. (Conclusion, Paragraph 87)
23. The models suggested by the National Police Chiefs Council are both potential ways to improve the senior oversight and consistency of policing crimes targeting MPs and candidates, but do not go far enough. Even with more central coordination it will still be challenging for local forces to develop the understanding of the democratic and political issues involved

when these crimes are relatively uncommon. Ultimately to deliver this, a dedicated unit for investigating anti-democratic crimes will be required. (Conclusion, Paragraph 95)

24. To drive consistency, the Government should work with policing to begin a phased process towards establishing a centralised, senior-led unit to investigate anti-democratic crimes, which would include abuse and intimidation of MPs and candidates as well as abuse of other elected officials and related issues like transnational repression. This approach would ensure that policing had the expert capability required to tackle these unusual crimes that it is not cost-effective for local forces to develop. The responsibilities for the protection of MPs and candidates, as well as sites and events of democratic importance, such as homes and offices and campaign meetings, would remain with the relevant local police forces. Responsibility for public order and protests would also not change. The new model should have clear mechanisms to determine what does and does not constitute an anti-democratic crime (in particular ensuring that crimes where the perpetrator did not know or consider that the victim was an MP are not wrongly considered anti-democratic) and the ability to join up local knowledge and specialist expertise. This should include knowledge of differences in legislation between the nations of the UK. It should also have an emphasis on intelligence and digital capabilities and a focus on nominal management and other preventative opportunities. (Recommendation, Paragraph 96)
25. The new unit should be introduced in a phased approach, beginning with the NPCC establishing a portfolio under the model of existing programmes like the National Police Coordination Centre to provide intelligence support, coordinate the national response, and develop and monitor adherence to clear national guidance and minimum standards for anti-democratic crimes. Initial stages should build on the existing efforts of PLaIT and Op Bridger to improve consistency and focus on ensuring senior ownership of threats against MPs and Parliamentary candidates, bringing forces in line with advice and guidance and delivering intelligence. Op Ford, which performs a similar function for other elected officials, should subsequently be included in the same programme: integrating Op Bridger and Op Ford should improve the intelligence capability but the currently unknown demand from Op Ford is likely to be a significant driver of cost. The capability should be appropriately resourced at all stages: in particular there must be sufficient understanding of Op Ford's resource needs as well as additional funding and staffing before any integration occurs to ensure that coordination does not result in existing Op Bridger resources being diverted to Op Ford. Once established, the unit should take responsibility for investigating crimes that target politicians because of their roles, and other anti-democratic crimes. (Recommendation, Paragraph 97)

- 26.** From an early stage, the NPCC's aim and responsibility should be to ensure that police forces' investigations into criminal threats against MPs and candidates follow national guidelines, to bring in external stakeholder and coordinated policing resources to deal with crises, and to develop the shared intelligence and preventative measures to stop threats escalating. This should include ensuring forces fully implement the Defending Democracy Policing Protocol's provisions on ensuring that protests at constituency offices do not impede the use of the venue or threaten or abuse attendees; and taking the lead on developing and disseminating the guidance to clarify criminal thresholds which we recommended in our first report. This guidance should include advice to local forces on when it would be appropriate to consider investigating threats against an MP or candidate as terrorism, what powers and capabilities would be available to do this and how to seek advice from the NPCC lead on when to refer a case to Counter-Terrorism Policing. This advice should acknowledge the unique history and security situation in Northern Ireland. In order to ensure counter-terrorism powers are used appropriately, the NPCC lead should establish a dedicated liaison and good working relationship with the Counter-Terrorism Policing network. (Recommendation, Paragraph 103)
- 27.** In line with our previous recommendation, elections law policing should, in future, be brought within the remit of the anti-democratic crimes unit. Until then, current arrangements for ensuring each police force has electoral law expertise are still very necessary. However, candidates are now far more likely to be affected by abuse and intimidation than elections law crimes. The expertise of their named point of contact should reflect this. We therefore recommend that Op Bridger leads and Force Elected Official Advisers (FEOAs) should be candidates' named points of contact. The elections single points of contact (SPOCs) should understand the issue of harassment at elections and how to refer anyone affected by it to the Op Bridger lead or FEOA. The NPCC should ensure that the Op Bridger leads, FEOAs and elections single points of contact are joined up and share knowledge and intelligence, at both local force and national leadership levels. (Recommendation, Paragraph 106)
- 28.** For decisions on whether or not to prosecute criminal threats against MPs and candidates to be consistent the harm they do to democracy must be consistently accounted for as part of the public interest test. Acknowledging that these cases are damaging but rare, the Crown Prosecution Service (CPS) has put in place measures to ensure senior oversight of prosecutions, although most are still handled at the local level. However, consistent decision making is a function of expertise, not seniority, and it would be more effective to have a small team of specialists focused on prosecuting

anti-democratic crimes and expertise in electoral law to ensure consistent assessments of the public interest in prosecution of such cases. (Conclusion, Paragraph 112)

29. Prosecutors can inform their assessment of the public interest of prosecuting with the community impact statement for crimes against MPs provided by the Speaker of the House of Commons. However, this statement does not currently cover candidates or MPs' staff. Reflecting the risk that both face from anti-democratic crimes, the Speaker will work with the Director of Public Prosecutions and the police to expand, or produce new statements, that can be considered as part of the public interest test for crimes against candidates or MPs' staff. (Conclusion, Paragraph 113)
30. The lack of available data makes it hard to assess the effectiveness of the CPS's approach to ensuring consistency in prosecution thresholds. The Government, through the Defending Democracy Taskforce, must begin to collect 'full picture' data on criminal cases targeting elected officials because of their roles. The Ministry of Justice should be represented on the Defending Democracy Taskforce at ministerial level to reflect the need for a full criminal justice system grip on this issue. Building on the current CPS central oversight of cases involving MPs, a system should be established to track cases referred to CPS, and the charging and sentencing outcomes, as well as applications for protective orders (covered below). The data should be used to identify inconsistency in decisions, which can be used to inform CPS guidance, target training and advice, and help determine the appropriate level of central CPS oversight. The data gathered should also be shared with police and the Parliamentary Security Department on an ongoing basis. (Recommendation, Paragraph 114)
31. MPs are entitled to decide who they and their staff will meet or otherwise engage with. In cases of stalking or harassment protective orders play an important role in ensuring the sense of safety of MPs and their staff. It is therefore unsatisfactory to assume they will be imposed without a mechanism to ensure it, especially as courts may well have concerns about preventing an individual from contacting their MP. (Conclusion, Paragraph 119)
32. The Sentencing Council and devolved equivalents should produce guidance on protective orders in cases where the perpetrator has targeted an MP or their staff. Guidance should include:
 - a. The presumption that a protective order should be imposed, in recognition of MPs' vulnerability due to their public prominence and regular engagement with the public, and staff members' vulnerability due to their public facing role and easily identifiable working location.

- b.** Where the perpetrator is a constituent of the MP, a mechanism for how they can still avail themselves of a right to be represented in Parliament without causing risk or alarm to the victim, such as passing communications through an intermediary. (Recommendation, Paragraph 120)
- 33.** As technology is developed to assist police with enforcement of domestic violence protection orders, the Government should explore how this can be used to help frontline police officers enforce restraining orders, stalking protection orders and other court orders intended to prevent people harassing MPs. As noted in our first report, MPs and candidates should be kept informed about key developments that may affect their sense of safety, such as a protective order being imposed or removed, or the perpetrator being released from prison. (Recommendation, Paragraph 121)
- 34.** Parliament should also support efforts to ensure the enforcement of protective orders. The House service should accelerate plans for a visitor information system. Whilst improving visitor experience, this system will provide an important mechanism to check the identity of visitors to the Parliamentary estate to ensure that individuals who are prohibited from approaching their MP by a protective order are not able to use Parliamentary access to do so. (Recommendation, Paragraph 122)
- 35.** The CPS and the courts have provisions in place for expediting trials in cases that occur during election periods and which may affect or disrupt the outcome. However, these provisions do not appear to be widely used or effective, as many cases are still not resolved until long after the end of the election campaign. The Government and the CPS should set new targets for prosecutors and courts such that all cases of intimidation and abuse of candidates that occur during an election period, and have a reasonable chance of successful prosecution, should be dealt with within days in order to minimise the risk of them influencing the vote. (Conclusion, Paragraph 125)
- 36.** Our first report said we would consider the merits or otherwise of a) a specific offence against MPs and b) an aggravating factor applicable to sentencing for crimes committed against candidates or MPs because of their role. It is clear that there is a case for a specific aggravating factor and that this has advantages over a specific offence because it would be better able to take account of the various ways people may try to intimidate a politician. (Conclusion, Paragraph 132)
- 37.** We therefore welcome the Government's decision to introduce a new statutory aggravating factor for offences motivated by hostility towards candidates, campaigners, elected representatives, or electoral staff. The Government should ensure this can be applied broadly, including covering crimes that are motivated by hostility to elected officials but directed

against their staff and representatives, who are often on the front line of abuse and intimidation of MPs. To this end, we recommend the Government bring forward legislative proposals, at the earliest opportunity, that reflect the elements and spirit of the draft legislative provisions we have included at Annex 3. Governments of the devolved nations should take steps to reflect this change in their own legislation. (Recommendation, Paragraph 133)

38. Abuse targeted at female MPs and candidates remains a particular issue. Sex remains the only protected characteristic not covered by the protections of hate crime legislation or aggravating factors at sentencing. The debates around how hate crime legislation might cover misogynistic abuse of this kind are complicated and could have significant impact on women across the country. The Government should review the findings of the Law Commission, as well as the Scottish and Northern Irish studies, about making misogyny an aggravating factor. The political parties should recognise that the challenge of misogynistic abuse is unlikely to be resolved soon or easily and offer tailored support to their female officials and candidates to reflect the additional pressure they are likely to be under. (Recommendation, Paragraph 136)
39. In our first report we recommended that police forces should plan for "the potentially higher risk profile some candidates may have, either carried over from their time as an MP, because of their own prominence, or for other factors affecting their level of risk, whilst ensuring no political advantage is given to any candidate": for the sake of clarity we confirm that this should include considering the greater risks of abuse and intimidation female candidates are likely to face, especially online. (Recommendation, Paragraph 137)
40. When individuals are convicted of political intimidatory offences, the courts are required under the Elections Act to impose electoral disqualification orders, which bar them from standing for relevant elected roles for five years. There is a worrying lack of awareness and understanding about electoral disqualification orders, and indications that courts may be consistently omitting to impose them. Although these really affect only the small number of perpetrators who might wish to stand for election, the confusion around them reflects a lack of care and prioritisation of an important issue: the ability to stand for election is a valuable democratic right, and when it has been forfeited there must be certainty that that penalty will be consistently imposed to avoid any inequity or uncertainty about whether a candidate can stand. (Conclusion, Paragraph 140)
41. Before the Government carries out the review we have recommended of the effectiveness of disqualification orders, it should take immediate measures to ensure they are actually being used. The Crown Prosecution Service should instruct prosecutors to inform courts of their powers to use

a disqualification order whenever relevant. The Sentencing Council, Scottish Sentencing Council and Court of Appeal in Northern Ireland should ensure that judges are aware of these orders, by updating sentencing guidelines, guideline judgements or guidance as appropriate. The Government should confirm in its response to this report that these steps have been completed or action taken to complete them within the next year. (Recommendation, Paragraph 141)

Social Media

42. Social media platforms can be useful tools for MPs and candidates, and we anticipate that the part they play in facilitating engagement with constituents and voters is here to stay. However, these platforms are all private commercial products and are not designed or operated to have a specific political function. As such they form no part of the Fourth Estate, which we have acknowledged in Chapter One is a core pillar of democracy, and have no constitutional role. The impression held by some people, including some MPs, that MPs are required to make themselves available to their constituents on social media platforms is entirely false. MPs have as much right to decide who they and their staff engage with online as in person or by other means, and there is no requirement or convention for an MP to use a social media platform to send or receive communications. Moreover, unless there is a radical change in how social media companies treat political conversations and users, no such convention should be allowed to evolve. (Conclusion, Paragraph 148)
43. Currently only a few social media platforms are regularly used by candidates and MPs for their work, and, of those that are, the levels of abuse on the platforms vary significantly. We have therefore paid particular attention in the remainder of the chapter to the social media platforms that are the main source of threats to MPs and candidates: Facebook and X. However, patterns of social media use are likely to change, especially if the platforms fail to keep users safe from abuse, and we therefore encourage other social media platforms to learn from the lessons we have identified, in particular the greater risk of abuse faced by political figures and the greater care that must be taken to prevent it. (Conclusion, Paragraph 149)
44. The benefits social media bring to political engagement come at the significant cost of innumerable online threats against MPs and candidates. It falls disproportionately on female and ethnic minority politicians, who are more likely to be abused online relative to their white, male counterparts. The cost continues to rise, as social media platforms tolerate more and more content that would previously have been deemed unacceptable under their terms of service. Whilst MPs and their staff pay the price directly, everyone is indirectly affected because of the damage online abuse is doing

to political discourse. The development of Artificial Intelligence will only compound these costs, while at the same time being a necessary tool for addressing the issue. (Conclusion, Paragraph 160)

45. Although individual MPs and candidates do not have the power to solve the problem of online abuse, to keep themselves and their staff safe, and to preserve the quality and civility of online discourse, they should all actively engage the protective tools available to them on the social media platforms they use, such as ignoring or restricting replies and automatic filtering of offensive language. Additionally, they should block, screen or filter content from accounts that have not verified their identity, once this function is implemented under the Online Safety Act 2023. They should act swiftly to block any users, including constituents, who they feel are engaging in an abusive or aggressive manner. By reducing opportunities for individuals to post abusive and intimidatory content online, MPs and candidates will help to defuse the "toxic spiral of hate" that drives ever more abuse, exposes other users on the platform to inappropriate and distressing content, and dissuades people from standing for public office. (Recommendation, Paragraph 161)
46. MPs and candidates should feel empowered to leave any platform they judge to present a greater risk than benefit to their work. If political parties require candidates to post on specific social media platforms they should assess the risks and benefits of doing so for each individual candidate, carefully considering the political and personal factors that affect the chance the candidate will be abused. (Recommendation, Paragraph 162)
47. Relying on MPs and candidates to protect themselves on social media places a greater burden on groups more at risk of abuse, typically women and politicians from ethnic minority backgrounds, and can make it harder for them to campaign by reducing their engagement with the public. To avoid an unintentional discriminatory effect, it would be best if all MPs and candidates use all the protective measures available to them boldly and consistently. (Conclusion, Paragraph 163)
48. Although we encourage MPs and candidates to use the available tools to counter abuse, this will only go so far. For as long as people continue to use social media as a mouthpiece for abuse, true responsibility for resolving the issue of threats on social media lies with the platforms that host them. (Conclusion, Paragraph 164)
49. Although Meta and X's engagement on this issue during this inquiry has raised serious questions about their sincerity and determination to tackle it, they have recognised that they have responsibilities to their users and to democracy and are putting in place measures to mitigate abuse. These should be welcomed and expanded. In particular, Meta must engage better with smaller parties and offer them the same direct engagement enjoyed

by the larger parties. X provides a generic email address to the Electoral Commission to be shared with parties and candidates: it would be more effective for them to use the same model as Meta of a central liaison with parties. X should also return to its old policy, currently still used by Meta, of deploying automated messages to warn people when the content they are about to post may be abusive and contrary to the platform's policies. These nudges should be used more widely. For example, similar messages to those that users receive when they engage with creators on Facebook should also be used when contacting MPs or other elected officials, telling users that they are about to contact an elected representative, noting the importance of free speech and robust debate, but warning that threats and abuse undermine democracy, make it harder for politicians to represent their constituents, and are often illegal. (Conclusion, Paragraph 171)

50. As much of the abuse MPs receive comes through the Parliamentary email system, Parliament should explore whether to introduce automated prompts asking users to reconsider potentially abusive messages. As part of this exploration, the Parliamentary Digital Service (PDS) should consider alternatives to email, such as moving to an online contact form for MPs, as is the model in other legislatures, or systems such as contact portals or gateways, which could allow two-way dialogue between recipient and sender. These approaches could allow for the introduction of a prompt when people try to submit a potentially threatening message, inviting them to reconsider, while still allowing them to send the original message if they wish to. As part of its exploratory work, PDS should consider whether such an approach would make it easier: to process and screen messages for abusive content, to ensure messages are directed to the correct MP, to improve ability to manage the increasing volume of email received by MPs, and to implement the kind of behavioural nudge described above. It must consider that constituents' messages will often contain heightened emotional language which is expressive not threatening, and how to preserve the important human aspect of the nature of communications between MPs and their constituents. Any change of approach should be balanced with the need to maintain appropriate filtering, anti-spam and security measures, digital accessibility and MPs' offices' autonomy to manage responses and casework. Any proposed solution should be informed by clear political direction and consensus, with MPs being consulted as part of the development of any new system. Proposals should be presented to the House of Commons Administration Committee in time for consideration ahead of the next Parliament. (Recommendation, Paragraph 173)

51. In the meantime, PDS should work to increase awareness among MPs of the current optional facilities for screening emails for abuse and consider introducing banner-style messages for recipients on emails received containing potentially abusive content, signposting to appropriate reporting and support mechanisms. (Recommendation, Paragraph 174)
52. Despite the steps Meta and X have taken to mitigate some of the problems with abuse on their platforms, abusive content continues to be an issue. Their failure to address the larger underlying issues that drive abuse demonstrates that they do not properly understand the damaging impact they are having on democracy in the UK. We are particularly concerned about their unwillingness to remove abuse against MPs, candidates and other public figures; indications that X and Meta's algorithmic recommendation systems appear to give preference to incendiary and threatening content but with no recourse for independent review to assess this risk; and challenges the police and criminal justice system appear to face in obtaining information from X. We have no faith that Meta and X will resolve these issues unless they are legally obliged to do so. There is therefore no point in us recommending wholesale change of policies or modus operandi. The only viable solution is for Ofcom and the Government to compel them to protect their users. Currently, this will be via the Online Safety Act 2023. But should that legislation fail to tackle the root issues that influence the level of abuse and intimidation on social media platforms, further legislation will be needed. We return to this point in the final part of this Chapter. (Conclusion, Paragraph 186)
53. Meta and X's greater tolerance for abuse against MPs, candidates and other public figures is a particular challenge. Both platforms are unwilling to properly assess and remove clearly inappropriate content; we doubt this is even possible for X given its disproportionately small content management team. (Conclusion, Paragraph 187)
54. We agree that it can be hard to tell whether a threat made on social media against a public figure is real. Part of the challenge is that some threats may be used metaphorically or hyperbolically, but still add to a febrile political environment. We hope that the discussions between the Speaker, the parties and the Electoral Commission on a campaigning code of conduct will help to shape public understanding of the line where robust political discourse tips into inappropriately aggressive language. (Conclusion, Paragraph 188)
55. However, taking refuge in this complexity, as platforms do, misses the point. Having higher bars for removing threats against politicians normalises the idea that MPs and candidates should be expected to endure a greater level of abuse than people in other professions: this impression puts people off running as candidates and is damaging democracy. Platforms' use of

convoluted distinctions about whether a threat is “credible” or “severe” are an abdication of their responsibilities. We foresee the very real risk that these responsibilities will only be brought home to them in the worst way imaginable: when their assessment of the credibility of a threat is wrong, and they fail to remove content that instigates an attack. (Conclusion, Paragraph 189)

56. The statutory requirement for platforms to remove illegal content covers threats against MPs, candidates and other public figures, just as much as anyone else. In order to ensure that these threats are properly dealt with, Ofcom should pay particular attention to whether platforms' content moderation procedures introduce additional criteria relating to the removal of illegal content related to public figures when it reviews them under the Online Safety Act 2023. They should specifically consider whether these additional criteria breach provisions of the Act around requirements for systems to remove illegal content and to enforce the platform's policies consistently. The Government should review the US-UK Data Access Agreement in consultation with the police to establish whether it is effective in granting police the access to information they need from social media platforms about criminal activities. (Recommendation, Paragraph 190)
57. It is also important that, while abusive content remains on a platform, it is not promoted to other users, which can increase the harm to the victim and run the risk of triggering further abuse. The best defence against this is careful scrutiny of the platforms' recommendation algorithms by researchers and Ofcom. The Government should design and implement an access to data regime that delivers maximum transparency around platforms' operations. (Recommendation, Paragraph 191)
58. The Online Safety Act 2023 has the potential to deal with many of the issues of online threats to MPs and candidates that we have identified. In particular, it could force platforms to properly resource their content moderation teams, remove illegal content, and grant some oversight of how their content recommendation algorithms function. (Conclusion, Paragraph 198)
59. However, whether or not it does so will depend on how it is implemented. For the sake of the affected individuals and democracy as a whole, the abuse targeting MPs and candidates that has become commonplace on platforms must stop, and we are encouraged to hear that Ofcom is focused on this as a measure of success. Phase 3 has the potential to give MPs, candidates, and other users an opportunity to operate free from abuse, which we encourage everyone to seize. However, that opportunity will only materialise if Ofcom makes full use of all the regulatory powers it has been given under the Act. (Conclusion, Paragraph 199)

- 60.** In order to ensure that the Act meets the aspirations Parliament had for it once fully implemented, Parliament must continue to have a say in its implementation. The processes for approval for implementation of the Online Safety Act make it challenging for parliamentary committees to scrutinise codes of practice in an effective and timely manner. Whilst two thirds of the Act is now in force, there remains an opportunity for Parliament to engage in the implementation of the third phase and in any future revisions. As the Act comes into force it is also vital that Parliament has the opportunity to assess its effectiveness. Ofcom must make available to Parliament the information to facilitate this scrutiny.
- Ofcom should facilitate scrutiny by keeping the relevant parliamentary committees well-informed of upcoming milestones, including notifying them of consultations, codes being sent to the Secretary of State for approval, and anticipated windows for parliamentary engagement and scrutiny.
 - Ofcom must lay a bi-annual report before Parliament, which we encourage the relevant parliamentary select committees to engage with. This report should set out, as a minimum:
 - data and updates on i) compliance and ii) investigative/enforcement action; and
 - Ofcom's assessment of the Act's impact on i) platform behaviour and ii) user experience. (Recommendation, Paragraph 200)
- 61.** Ofcom must be given time to fully implement the Online Safety Act, in line with the recommendations made above. However, given how central social media is to the issue of threats against MPs and candidates, as well as so many areas of public and private life, it is unlikely that this is the last legislation Government will need to pass on social media regulation. Given the exceptionally complex, technical and politically charged nature of this topic, preparations should be made ahead of time so that options for further regulation are ready for the Government to act on when needed. (Recommendation, Paragraph 204)
- 62.** These preparations should take account of the fact that political discourse online drives more abuse than other topics and should therefore include consideration of what additional protections platforms may need to put in place around political discussions. These may include prohibiting platforms from having different standards for removing threats against politicians and other public figures, or requiring the introduction of automated prompts like those we called for above, to warn users if they are about to post content that may be abusive, or to encourage them to engage appropriately when contacting an elected representative. (Recommendation, Paragraph 205)

- 63.** 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. (Recommendation, Paragraph 206)
- 64.** The Government should also note the amount of work required of Ofcom to regulate such a large and evolving sector and prioritise ensuring that it is properly resourced to take on this task. (Recommendation, Paragraph 207)
- 65.** The Conference's first report noted issues with the enforcement of section 106 of the Representation of the People Act 1983 and recommended the Government review how to make the intention behind it enforceable. False statements of this kind are a particular concern when shared online: we therefore recommend that the Government give appropriate consideration to how any updated legislation can be enforced against online disinformation. As part of this work, and in order to ensure the same issues with enforcement are not repeated, the Government should review the enforcement and effectiveness of the false communications offence introduced by the Online Safety Act 2023. In line with the recommendation in our first report, and in order to address the terrible spread of sexually explicit deepfakes targeting female candidates, the Government should ensure that current legislation and any amended legislation on false statements about candidates explicitly cover the creation of deepfakes. (Recommendation, Paragraph 213)
- 66.** Doxing and pile-on harassment cause significant distress but are not sufficiently addressed by existing legislation. The Government should introduce legislation that is specifically designed to address these issues at the earliest opportunity. (Recommendation, Paragraph 217)

Conclusion

- 67.** Our reports have highlighted that tackling threats against MPs, candidates and elections will require a focused, co-ordinated effort across multiple organisations. We hope that the recommendations made in our two reports help shape an agenda for change that improves the current climate of abuse and intimidation affecting the daily lives of MPs, their staff and families, which causes significant harm to democracy. (Conclusion, Paragraph 225)

Appendix 1: 23rd Meeting of the Speakers of The Lower Houses of the G7 Declaration²⁹¹

1. We, the Speakers and Presidents of the lower houses of the G7 legislatures, along with the President of the European Parliament, met from September 4th to 6th, 2025, in Ottawa, Canada, and the surrounding region, to discuss global challenges confronting our countries. The themes of our meeting – online disinformation and the threat it poses to democratic processes, political polarization and its effects on legislative debates, and violence against legislators – reflect some of these global challenges.
2. Our 23rd Meeting reaffirmed the importance of parliamentary diplomacy as a means of fostering exchange, dialogue, and collaboration. We condemn Russia’s continuing aggression against Ukraine and recognize Ukraine’s readiness for a just and lasting peace. We endorse the March 14, 2025, Joint Statement of the G7 Foreign Ministers, which reaffirmed unwavering support for Ukraine in defending its territorial integrity and right to exist, and its freedom, sovereignty and independence. We reiterate our commitment to deepening our cooperation on issues of shared importance, and to strengthening the interparliamentary dimension of the G7. This joint declaration summarizes the outcomes of our deliberations.

A. ADDRESSING ONLINE DISINFORMATION AND THE THREAT IT POSES TO DEMOCRATIC PROCESSES

3. We recognize that the rapid advancement of artificial intelligence (AI), when coupled with the amplifying power of social media, has heightened the vulnerability of our voters to information manipulation and interference, including disinformation. Hostile actors and authoritarian regimes exploit

291 It is recognized that due to their constitutional positions or other factors, certain Speakers cannot directly associate themselves with substantive political statements, and therefore should not be seen as indicating specific support for all sections of this declaration. Nonetheless, on behalf of their Chambers, they recognize the importance of the issues raised and the intentions of their colleagues in proposing particular ways forward.

these technologies to interfere in our democratic processes. At the same time, we acknowledge that these technologies bring immense benefits across many sectors, driving innovation, productivity, and social progress.

4. Accordingly, we discussed how our respective legislatures have acted – and might act going forward – to strike the right balance: protecting our democracies and citizens from the risks posed by AI-driven information manipulation and interference, including disinformation, while fostering responsible innovation and upholding fundamental rights, including freedom of expression. We reaffirm our shared commitment to open dialogue, mutual learning, and coordinated action, in the interest of safeguarding democratic institutions and public trust in the digital age.

B. LEGISLATURES IN A POLARIZED WORLD: FOSTERING RESPECTFUL DEBATE IN THE CHAMBER AND BEYOND

5. We recognize that more of our citizens, especially young voters, appear to be losing faith in democratic institutions and gravitating towards extreme ideological positions.
6. We are particularly concerned about the link between extreme polarization and support for political violence. Social media and other online platforms, driven by opaque algorithms, are contributing to both by amplifying polarizing content aimed at sowing discord, and by reducing access to a diversity of content, notably by filtering out opposing political viewpoints. We encourage governments, legislators, the private sector and civil society to work together to promote digital, media and information literacy, civil discourse, constructive democratic debate and to counter online foreign influence.

C. PROTECTING LEGISLATORS FROM ALL FORMS OF VIOLENCE

7. We express grave concern over acts of violence against legislators. Legislators are exposed in two ways: as nationally elected officials with significant media visibility, and also because of their local presence, since they often have constituency offices. Internet and social media – tools that should be used for democratic engagement – have increasingly become vehicles for harassment and abuse targeting legislators and their private, family and professional lives.
8. We note that abuse against legislators, including online harassment and threats of violence, have profound consequences. These include deterring individuals from entering politics, driving legislators to leave public life, influencing how democratic work is carried out, and limiting the perspectives that are represented in legislatures. This behaviour is on the

rise, and we condemn the troubling trend. We reaffirm our commitment to upholding the right of all individuals to participate fully and equally in public life.

9. Legislators must be able to fulfill their duties in environments free of violence and harassment, both within and beyond their legislatures. Strengthening the legislative framework to better prevent and punish violence against legislators is necessary. We are committed to doing our part to prevent and eliminate such behaviour.

Canada

The Honourable Francis Scarpaleggia

Speaker of the House of Commons of Canada

France

Her Excellency Yaël Braun-Pivet

President of the National Assembly of the French Republic

Germany

Her Excellency Julia Klöckner

President of the German Bundestag

Italy

His Excellency Lorenzo Fontana

President of the Chamber of Deputies of the Italian Republic

Japan

His Excellency Fukushima Nukaga

Speaker of the House of Representatives of Japan

(in absentia)

United Kingdom

The Right Honourable Sir Lindsay Hoyle

Speaker of the House of Commons of the United Kingdom

United States of America

The Honorable Mike Johnson

Speaker of the House of Representatives of the United States of America

European Union

Her Excellency Roberta Metsola

President of the European Parliament

Formal minutes

Wednesday 15 October 2025

Members present

Sir Lindsay Hoyle, in the Chair

Lee Anderson MP

Kirsty Blackman MP

Zöe Franklin MP

Dr Rupa Huq MP

Leigh Ingham MP

Jessica Morden MP

Rebecca Paul MP

John Slinger MP

Sir Mark Tami MP

Sir Jeremy Wright MP

Speaker's Conference on the security of candidates, MPs and election

Draft Report (Speaker's Conference on the security of candidates, MPs and elections), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 225 read and agreed to.

Annexes and Summary agreed to.

A Paper was appended to the Report as Appendix 1.

Resolved, That the Report be the Second Report of the Conference to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available (Standing Order No. 134).

Ordered, That the following correspondence be reported to the House for publication:

Letter, dated 23 September 2025, from Dan Jarvis MBE MP, Security Minister to the Speaker relating to terrorism legislation

Adjournment

The Committee adjourned.

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the [inquiry publications page](#) of the Committee's website.

Wednesday 5 February 2025

Ellie Reeves MP, Chair, Labour Party; **Andrew Whyte**, Executive Director, Governance and Legal, Labour Party; **Bob Blackman MP**, Chair 1922 Committee, Conservative Party; and **Stephen Massey**, Former Chief Executive Officer, Conservative Party

[Q1-17](#)

Jeremy Corbyn MP, Independent; and **Iqbal Mohamed MP**, Independent

[Q18-22](#)

Mike Dixon, Chief Executive Officer, Liberal Democrats; and **Elfrede Brambley-Crawshaw**, Elections Manager, The Green Party

[Q23-36](#)

Owen Roberts, Chief Executive Officer, Plaid Cymru; **Timothy Johnston**, Chief Executive, DUP; and **Colin McGrath MLA**, Chair, SDLP

[Q37-44](#)

Wednesday 26 February 2025

Vijay Rangarajan, Chief Executive, Electoral Commission; **Peter Stanyon**, Chief Executive, Association of Electoral Administrators; **DCI Kevin Ives**, National Co-Ordinator for Election Crime, City of London Police; **Niki Nixon**, Interim Director of Communications, Electoral Commission

[Q45-76](#)

Will Fletcher, Interim CEO, The Jo Cox Foundation; **Professor Helen Margetts**, Professor of Society and the Internet, Oxford University; **Dr Sofia Collignon**, Senior Lecturer in Comparative Politics, Queen Mary University of London

[Q77-96](#)

Wednesday 12 March 2025

Detective Inspector Lee Barnard MBE, Operational Lead, Parliamentary Liaison and Investigation Team (PLaIT), **Steve Jones**, Lead Analyst, Parliamentary Liaison and Investigation Team (PLaIT), **Chief Inspector Bryan Duffy**, National Strategic Bridger Lead and **Simon Messinger**, Commander, Protection

[Q97-122](#)

Alison Giles CB, Director, Parliamentary Security Department and **Oliver Davis**, Deputy Director (Members' Security and Risk), Parliamentary Security Department [Q123-146](#)

Wednesday 2 April 2025

Dan Jarvis MBE MP, Minister for Security, Home Office; **Shaun Hipgrave**, Director Protect and Prepare, Home Office; **Rushanara Ali MP**, Minister for Homelessness and Democracy, Ministry of Housing, Communities and Local Government; **Becca Crosier**, Deputy Director for Elections Strategy, Ministry of Housing, Communities and Local Government [Q147-170](#)

Wednesday 4 June 2025

David Hughes, Chair, Parliamentary Lobby; **Anushka Asthana**, Chair, Parliamentary Press Gallery [Q171-197](#)

Liz Moore, Chief Executive, Association for Citizenship Teaching; **Professor Helen Fenwick**, Professor of Human Rights Law, Durham Law School; **Karthik Ramanna**, Professor of Business and Public Policy, Blavatnik School of Government; **Elisabeth Costa**, Chief of Innovation and Partnerships, Behavioural Insights Team [Q198-211](#)

Wednesday 2 July 2025

Chief Constable Gavin Stephens, Chair, National Police Chiefs' Council; **Nick Price**, Director of Legal Services (interim), Crown Prosecution Service; **The Hon. Lord Colbeck**, Judicial Member, Scottish Sentencing Council [Q212-240](#)

The Rt Hon. Dame Diana Johnson MP, Minister of State (Minister for Policing and Crime Prevention), Home Office; **Lucy Rigby KC MP**, Solicitor General; **Sarah Sackman KC MP**, Minister of State, Ministry of Justice [Q241-270](#)

Wednesday 9 July 2025

Claire Dilé, Government Affairs Director, Europe, X (formerly known as Twitter); **Megan Thomas**, UK Public Policy Manager, Meta; **Patrícia Rossini**, Senior Lecturer in Communication, Media & Democracy, University of Glasgow [Q271-345](#)

Wednesday 3 September 2025

Jessica Zucker, Director of Online Safety Policy, Ofcom; **Almudena Lara**, Director of Online Safety Policy, Ofcom; **Mark Bunting**, Director of Online Safety Strategy, Ofcom

[Q346–390](#)

Tuesday 9 September 2025

Talitha Rowland, Director for Security and Online Harms, Department for Science, Innovation and Technology; **Kanishka Narayan MP**, Minister for AI and Online Safety, Department for Science, Innovation and Technology

[Q391–404](#)

Published written evidence

The following written evidence was received and can be viewed on the [inquiry publications page](#) of the Committee's website.

SCS numbers are generated by the evidence processing system and so may not be complete.

1	50:50 Parliament	SCS0036
2	Addressing Candidate Security in Contemporary Election Campaigns Banducci, Susan (Professor, University of Birmingham); Tyler, Professor Katharine (Professor, University of Exeter); Fagin, Dr Jessica (Postcortical Researcher, University of Sheffield); Blamire, Dr Joshua (Research Fellow, University of Wolverhampton); Castro, Dr Alejandro Tirado (Postdoctoral Researcher, CSIC, Spain); and van Zijl, Julia (PhD Researcher, University of Birmingham)	SCS0030
3	Anonymised	SCS0044
4	Anonymised	SCS0043
5	Anonymised	SCS0033
6	Antisemitism Policy Trust	SCS0006
7	Association for Citizenship Teaching (ACT)	SCS0050
8	Association of European Threat Assessment Professionals	SCS0029
9	Association of Police and Crime Commissioners (APCC)	SCS0019
10	BCS, The Chartered Institute for IT	SCS0025
11	Behavioural Insights Team	SCS0052
12	Campbell-Savours, Lord	SCS0035
13	Center for Countering Digital Hate (CCDH)	SCS0028
14	Clean up the Internet	SCS0007
15	Collignon, Dr Sofia (Senior Lecturer in Comparative Politics, Queen Mary University of London)	SCS0041

16	Collignon, Dr Sofia (Senior Lecturer in Comparative Politics, Queen Mary University of London); Rüdig, Dr Wolfgang (Reader in Politics, University of Strathclyde); and Banducci, Professor Susan (Professor in Political Science, University of Birmingham)	SCS0023
17	Committee on Standards in Public Life	SCS0012
18	Compassion in Politics	SCS0034
19	Crown Prosecution Service	SCS0024
20	Khan DBE, Dame Sara	SCS0039
21	Danczuk, Mr Simon	SCS0021
22	Electoral Commission	SCS0049
23	Electoral Commission	SCS0020
24	Full Fact	SCS0056
25	Glitch	SCS0018
26	Harmer, Dr Emily (Senior Lecturer in Media , University of Liverpool); and Southern, Dr Rosalyn (Senior Lecturer in Political Communication , University of Liverpool)	SCS0017
27	Hogan Lovells International LLP	SCS0038
28	Home Office	SCS0042
29	Joint Committee on Human Rights (UK Parliament)	SCS0037
30	King, Florence (PhD Researcher, Swansea University)	SCS0015
31	Maynard, Dr Diana (Senior Research Fellow, University of Sheffield); and Bontcheva, Professor Kalina (Professor, University of Sheffield)	SCS0014
32	Members' and Peers' Staff Association (MAPSA)	SCS0032
33	Meta	SCS0054
34	Metropolitan Police	SCS0048
35	Metropolitan Police	SCS0047
36	National Police Chiefs' Council (NPCC)	SCS0051
37	Online Safety Act Network	SCS0001
38	Perry, Professor Barbara (Professor, Ontario Tech University)	SCS0003
39	Parliamentary Security Department	SCS0046
40	Parliamentary Security Department	SCS0045
41	Public Prosecution Service	SCS0013

42	Renwick, Professor Alan (Professor of Democratic Politics and Deputy Director of the Constitution Unit, University College London)	<u>SCS0031</u>
43	Reset.Tech	<u>SCS0004</u>
44	Scottish Sentencing Council	<u>SCS0022</u>
45	Sentencing Council	<u>SCS0005</u>
46	Sentencing Council for England and Wales	<u>SCS0053</u>
47	Shair-Rosenfield, Dr. Sarah (Professor, University of York); Davies, Dr. Graeme (Professor, University of York); Johns, Dr. Robert (Professor, University of Southampton); and Wood, Dr. Reed (Professor, University of Essex)	<u>SCS0026</u>
48	Stephen, Mr. Michael (Conservative MP 1992–97, House of Commons)	<u>SCS0002</u>
49	The Jo Cox Foundation	<u>SCS0008</u>
50	Theseus Risk Management Ltd	<u>SCS0010</u>
51	Walney, Lord (UK Government’s Independent Adviser on Political Violence and Disruption, The Home Office)	<u>SCS0016</u>
52	X (formerly known as Twitter)	<u>SCS0055</u>

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the [publications page](#) of the Committee's website.

Session 2024–26

Number	Title	Reference
1st	Speaker's Conference on the security of MPs, candidates and elections	HC 570