

Speaker's Conference (2024)

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

First Special Report of Session 2024–26

HC 1709

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 10 February 2026, to be printed. It was published on 5 March 2026 by authority of the House of Commons.
© Parliamentary Copyright House of Commons 2026.

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 Committee's email address is Speakersconference2024@parliament.uk.

First Special Report

The Speaker's Conference on the security of MPs, candidates and elections published its [First Report of Session 2024–26](#), (HC 570) on 2 June 2025 and its [Second Report of Session 2024–26](#) (HC 1303) on 27 October 2025. The Government response to both reports was received on 22 December 2025 and is appended below, along with responses from the National Police Chiefs Council (NPCC); the Parliamentary Security Department (PSD); the Parliamentary Digital Service (PDS); the Parliamentary Education and Engagement Team; the Sentencing Council; the Electoral Commission and Ofcom.

The table below indicates the response, or responses, in which each recommendation is addressed.

Responses to the Conference's recommendations

First Report

		Parliamentary			External				
Para	Summary of topic	Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (p.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
8	Campaign code of conduct (c.f. second report para 188)				✓	✓			
29	Parties offer information and support				✓				

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (p.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
36	Default transfer of security from PSD to Home Office	✓			✓				
37	Monitor Disqualification Orders (c.f. Second Report para 141)				✓	✓			
45	Policing plans (c.f. Second Report para 137)				✓	✓	✓		
48	Reforms to candidate registration				✓	✓			
56	Code of practice for election officials				✓	✓			

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (p.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
57	Review of electoral law (c.f. Second Report para 213)				✓	✓			
69	PSD to flex arrangements to risk	✓			✓				
70	MPs' duty regarding security				✓				
71	MPs' duty of care to staff				✓				
80	Culture shift in criminal justice system				✓				
87	Clarity on criminal thresholds				✓		✓		

		Parliamentary			External				
Para	Summary of topic	Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (p.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
91	Proactive policing of harassment				✓		✓		
92	All incidents to be reported				✓				
94	Victims to be kept informed						✓		

Second Report

		Parliamentary			External				
Para	Summary of topic	Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
30	Citizenship education programme				✓	✓			

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
33	Supporting MPs' engagement with young people			✓	✓	✓			
34	UK Parliament Week			✓	✓				
35	Local councillors engaging young people			✓	✓				
44	Research motivations of perpetrators				✓	✓			
45	Public health-style campaign against abuse				✓				
55	Long-form interviews				✓				
59	Headlines				✓				
71	Doorstepping				✓				✓

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
75	Press approaching families				✓				✓
96	Central policing unit				✓		✓		
97	Phase approach to set up				✓		✓		
103	NPCC guidance to forces						✓		
106	Op Bridger and FEOAs as candidates' PoCs				✓	✓	✓		
112	Central prosecution unit				✓				
113	New community impact statement								
114	Collecting data on cases				✓				

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
120	Guidance on protective orders when offences target MPs				✓			✓	
121	Technology to enforce protective orders				✓		✓		
122	Parliamentary visitor ID system	✓			✓				
125	Targets for case times				✓				
133	Aggravating factor				✓	✓			
136	Government and political parties response to misogyny				✓				

		Parliamentary			External				
Para	Summary of topic	Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
137	Considering gender as risk factor in police risk assessment (c.f. First report para 45)						✓		
141	Ensure consistent implementation of Electoral Disqualification orders (c.f. First Report para 37)				✓	✓		✓	
161	Use of protective measures on social media				✓				
162	Leaving damaging social media platforms				✓				

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
163	All MPs to use social media protective measures								
173	Potential for measures to restrict harassment via Parliamentary email		✓		✓				
174	Increase MPs' awareness of email screening		✓		✓				
188	Code of conduct to cover hyperbolic threats (c.f. First Report para 8)								

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
190	Enforcement of laws against social media abuse and platforms' tolerance for abuse against public figures				✓	✓			✓
191	Access to data regime to assess spread of illegal content				✓	✓			✓
200	Parliament and implementation of Online Safety Act				✓				✓
204	Preparation for future social media regulation				✓	✓			

Para	Summary of topic	Parliamentary			External				
		Parliamentary Security Department (P.65 - 66)	Parliamentary Digital Service (P.67-68)	Education and Engagement (P.69-70)	Government (P.14-54)	Electoral Commission (P.75-88)	NPCC (P.55-64)	Sentencing Council (P.71-74)	Ofcom (P.89-96)
205	Consideration of how political discourse drives abuse online				✓	✓			
206	Consider elections code of practice for platforms				✓	✓			
207	Consider resourcing of Ofcom				✓				
213	False statements online (c.f. First Report para 57)				✓	✓			
217	Legislation on doxing and pile-on harassment				✓				

Note: House of Commons reports do not number recommendations separately from conclusions, and as a result numbering of recommendations varies between reports. The table therefore identifies them using paragraph numbers from the original reports.

Appendix 1: Government Response

Introduction

The UK Government thanks the Speaker's Conference for its reports on the security of MPs, candidates, and elections. This written response represents all relevant Government departments, Ofcom, and the Crown Prosecution Service. Police and Parliament will respond separately.

The Government supports the Speaker's Conference focus on threat reduction and is taking action on all key themes in its report: threats faced by candidates and MPs and the impact on democracy; the effectiveness of Government and policing responses during elections and to MPs' safety; public attitudes; the criminal justice response; and the response from social media companies.

This response addresses the issues identified by the Conference and outline steps already taken, as well as further actions following internal and external reports and reviews, to tackle harassment of elected representatives. This complements the Government's written submission and oral evidence provided by the Security Minister, the former Minister for Democracy, the former Policing Minister, and the Minister for Online Safety and Artificial intelligence.

The murders of Jo Cox and Sir David Amess were not isolated tragedies; they shocked Parliament and our democracy, leaving grief and fear that now shape political discourse. Robust debate is vital and must be protected, but abuse and intimidation have no place. At the last general election, over half of candidates faced abuse or intimidation, and nearly all MPs have experienced it. This is unacceptable.

No one should be deterred from standing for public office due to safety concerns. Harassment of politicians undermines democracy and risks silencing voices. Intimidation of voters, electoral staff, candidates, and campaigners - online or in person- is equally unacceptable and damages democratic participation.

We take these threats incredibly seriously. While protective measures exist, more must be done to ensure voters, candidates, and election staff feel safe. Serving as an elected representative is an honour and a privilege, and Government will do all it can to preserve both the safety and the sense of safety of those who serve.

The Defending Democracy Taskforce, chaired by the Security Minister, brings together Ministers, law enforcement, Parliament, the Electoral Commission, and the UK Intelligence Community. Its mandate, renewed by the Prime Minister, drives a whole-of-Government response to threats to democracy, with a key priority being the harassment and intimidation of elected representatives.

Significant progress has been made in the last decade. Parliament and Government have strengthened protective security and prosecution capabilities. Ahead of the last General Election, £31m was invested to boost police capacity and provide bespoke private security for those most at risk. The Taskforce continues to build resilience, track offenders, and defend democracy, including creating a dedicated team to counter harms targeting elected representatives.

Government has introduced new legislation through the Crime and Policing Bill to restrict protests at the homes of public office holders, recognising the impact on families and democracy. Additional Home Office funding supports a new police assessment team to improve intelligence gathering and consistency in responses to crimes against locally elected representatives. Guidance from the College of Policing will ensure clear investigative frameworks and use of powers.

The Ministry of Housing, Communities and Local Government has published its Strategy for Modern and Secure Elections - the boldest democratic reforms in decades. Measures include:

- A new aggravating factor in sentencing for offences targeting elected representatives.
- Expanded disqualification orders to protect electoral staff.

These changes reinforce that those who seek to undermine democracy will face serious consequences.

Abuse, intimidation, and personal attacks against elected representatives undermine democratic processes by limiting debate and discouraging individuals from running for office. Through the Defending Democracy Taskforce's leadership, this Government remains committed to tackling these harms.

Recommendation 1 (para 28, report 1)

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.

Response:

We welcome the Speaker's Conference's recommendation to establish a code of conduct for campaigning. We will work with the Speaker, the Electoral Commission, and political parties to develop a code which is fit for purpose, ensuring that it meets the needs of the broad range of candidates from across the political spectrum. We believe that it would be beneficial for the principles of the code to be in place in time for elections in May 2026 and encourage parties to engage quickly and productively with the Electoral Commission to facilitate this.

The Government agrees that leaders from across the political spectrum must be clear that there is no tolerance for intimidation and harassment in our democracy. This is a non-political issue which affects everyone and in which political leaders must be united in understanding the need to act. To ensure political debate is honest, transparent and remains civil and safe for all, campaigners must be accountable for their conduct.

An updated code of conduct will have a positive impact on the level of trust the public has in political parties, candidates, and campaigners, with more confidence that campaigns are being conducted with honesty and integrity and are not intentionally attempting to mislead the public. The Government recognises that the perception that threats and intimidation are becoming more acceptable within politics may be a driver of more widespread abuse. It is vitally important that candidates and elected representatives model the kind of robust but respectful debate which underpins our democracy.

Recommendation 2 (para 29, report 1)

They [political parties] 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 15 (para 92, report 1)

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 intimidating.

Recommendation 16 (para 94, report 1)

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.

Response:

It is vitally important that where elected representatives, candidates, voters or anyone else involved in the democratic process feels like a victim of a crime, that they report such abuse to the police.

There is additional support for some elected representatives, such as Op BRIDGER for MPs, and ahead of election periods the relevant guidance will be sent to candidates to explain the systems in place to support them. We support the idea that political parties provide guidance and other avenues to seek support when their members are victims of harassment.

It is vital that elected representatives and their staff feel encouraged and supported to report any threats of an abusive or intimidating nature they receive and we will continue to work with police to ensure a consistent response.

Effectiveness of the response: Elections

Recommendation 3 (para 36, report 1)

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.

Response:

For the first time ever, in the 2024 General Election, the Home Office provided a Private Security offering for all Parliamentary candidates called Op REGENCY. This formed part of a roll out of additional measures, such as an expansion of the Op BRIDGER network, and the creation of a Local Community Fund for the police to access during the election period.

These measures were all brought in as recognition of the increasing level of community tensions, and the potential risk candidates faced to their physical safety in the lead up to, and during, the General Election – This cumulated in the Home Office providing support for 532 events, to a total of 206 candidates.

This was a world leading offer, and we aim to continue to provide it to candidates for UK parliamentary elections going forwards.

The private security provision is not restricted to election periods. The Home Office provides Op REGENCY support to Ministers, and some locally elected representatives where it is assessed that the risk and threat facing them makes such support necessary and proportionate. Parliament also provide a private security offering for MPs who are not Ministers.

Recommendation 4 (para 37, report 1)

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 38 (para 141, report 2)

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.

Response:

Disqualification orders are a key tool to tackle harassment and intimidation. The Government agrees that it is vital that there is awareness of disqualification orders and that they are used consistently to ensure their effectiveness.

The Government agrees that for electoral law to be applied consistently, there must be broad awareness and understanding of all parts of it. We are working with His Majesty's Courts and Tribunals Service to obtain data on the use of disqualification orders and will consider the best method to make that data available, once this work is complete.

Subject to a full understanding of how disqualification orders are currently being used, we will engage with the Crown Prosecution Service, Sentencing Council for England and Wales, Scottish Sentencing Council and Court of Appeal in Northern Ireland to ensure that appropriate guidance is in place for prosecutors, judges and magistrates on these orders.

Recommendation 5 (para 45, report 1)

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.**

Response:

The police are a vital partner in providing safety to elected representatives both inside and outside of election time, that is why they sit on the Defending Democracy Taskforce as a key delivery partner. We know that police already create risk-assessed police plans in advance of election periods, and so Government agrees with the principal of this recommendation.

It remains the responsibility of the police to determine how to address this recommendation.

The National Police Chiefs Council national coordinator, Kevin Ives, when he was before the Conference referenced the need for better guidance for front line officers – who are often not specialist in electoral or democratic matters - so they know how best to police election related issues, this is something the Defending Democracy Taskforce is working with the College of Policing and NPCC to produce.

We have found, and as was recognised in the evidence provided to the conference, a key issue which needs resolving is the consistency of the police response. The guidance that is being developed, along with work being undertaken by the NPCC and Op BRIDGER network will help to address this.

The Security Minister met with senior police officers from the Metropolitan Police Service and NPCC in September and has written to Chief Constables, encouraging them to use all powers available to them to respond to incidents of harassment and intimidation of public office holders.

Recommendation 6 (para 48, report 1)

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.

Response:

Government recognises that ahead of the previous General Election, there were instances where there was difficulty in sharing the contact details of candidates with the police, slowing down their response in Op BRIDGER to supporting candidates. This issue was identified as part of the lessons learned exercise the Government – coordinated by the Joint Election Security and Preparedness Unit – conducted following the election.

In order to address this issue, the Government will make provision so that candidates will be able to complete and return an additional form with their nomination papers that will capture their contact details. This will be optional for the candidate. If the form is returned to the Returning Officer,

they will be required to send the contact details to the relevant local police force(s) so they can contact the candidate to invite them to security briefings for the election or for other security-related matters.

The contents of this additional form (and whether a candidate has or has chosen to return one) will not be viewable by the public or other candidates (unlike a number of other nomination forms which can be inspected in certain circumstances).

Recommendation 7 (para 56, report 1)

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 8 (para 57, report1)

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.**

Response:

The Government recognises the importance of ensuring that electoral law is fit for modern elections and we keep this under regular review. As announced in the Strategy for Modern and Secure elections, we are taking forward several changes to legislation which will improve protections for candidates, campaigners and electoral staff, and ensure that there are appropriate sanctions for those who abuse them. As such, we partially accept Recommendation 8.

A key part of strengthening the efficacy of existing electoral law is ensuring that electoral officials have the right guidance and support to carry out their roles and responsibilities relating to candidate and voter safety.

Electoral officials, such as Returning Officers, are independent officers. However, the Electoral Commission does produce Performance Standards and guidance for electoral officers. The Government is working closely with the Electoral Commission to ensure electoral officers have the right guidance, standards and support to tackle harassment and intimidation.

Candidate addresses

We agree with the principle of this recommendation that parliamentary candidates should not have their home address made public. Candidates can already choose to include a broader geographic area rather than their

address on ballot papers and most candidates already have the option to withhold their address being made public as part of the nominations process.

As announced in the Strategy for Modern and Secure Elections, we are making changes to the nominations process to better protect candidates who act as their own election agent. Under current legislation, election agents' addresses are published in the Notice of Election Agents. Unless candidates acting as their own election agents have an office address, it is their home address, which is published, even when the candidate has chosen to otherwise withhold it. This clearly puts candidates and their families at risk of violence and intimidation in their own homes. We will remove the requirement for candidates' home addresses to be published in the Notice of Elections Agents in these circumstances by giving them the option to provide a correspondence address.

The Government is clear that candidates should feel safe and secure in their homes and we will continue to review how their personal information is handled in the electoral process, including on ballot papers.

Candidate ID

To strengthen the integrity of the nominations process, the Government will introduce two new requirements for candidates standing for election:

- Candidates must provide proof of identity as part of the nominations process, ensuring they are who they say they are and helping to prevent impersonation or fraudulent nominations.
- Candidates must sign a new statutory declaration confirming they understand it is a criminal offence to knowingly provide false information on nomination papers.

These are proportionate measures designed to protect elections from candidates seeking to mislead the electorate or undermine the integrity of the democratic process.

Polling stations

It is vital that voters, candidates and electoral staff feel safe at polling stations. The undue influence offence ensures that voters are protected from harassment or pressure to change their voting intentions. Police can also use existing public order law to address behaviour which causes disruption outside polling stations.

The DDTF is working closely with the College of Policing to ensure that police are aware of how existing laws can be applied to tackle issues at polling stations. As set out elsewhere, Government is also working closely

with the Electoral Commission to ensure that electoral officers have the right guidance and support on how to ensure the safety and security of candidates and voters, including on polling day.

Clarifying scope of existing legislation

The Government agrees that it is vital that electoral law is fit for a modern electoral setting, and that it is clear and widely understood. Where this is not the case, we will take appropriate steps to update or clarify existing legislation. As set out elsewhere, we are working with the College of Policing and Electoral Commission to ensure that police and electoral officers have the right guidance on how to effectively apply electoral law and their respective roles in doing so, including how to address disturbances at election meetings or polling stations.

The Government recognises that there are potential issues with Section 106 of the Representation of the People Act 1983. We are reviewing how this legislation should apply in a modern electoral setting. Where necessary, we will take appropriate action to clarify the scope of Section 106, particularly to ensure that it captures emerging technologies (such as deepfakes and other AI technologies) and is future-proofed.

The Government does not believe that it would be appropriate to expand the scope of this offence beyond personal conduct and character, therefore capturing statements of a political nature. Robust political debate and freedom of expression is a fundamental part of our democracy. Including political statements within this offence would place a significant burden on the courts to act as de facto fact checkers during elections and would unnecessarily politicise the judicial system.

The Government continually assesses the effectiveness of electoral law. Where the law is found to be ineffective or outdated, Government will take appropriate action. As outlined in the Strategy for Modern Elections, we are making changes to legislation where necessary and taking steps to ensure that there is awareness of current electoral law and that it is applied effectively and consistently.

Effectiveness of the response: security of MPs

Recommendation 9 (para 69, report 1)

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 10 (para 70, report 1)

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 11 (para 71, report 1)

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.

Response:

This Government is clear that harassment and intimidation of those participating in public life has no place in our society and cannot be tolerated.

Harassment of people in public life is not something which stops when an election ends. It is an issue all year round, and our approach to the issue reflects that.

The Government's protective security system is rigorous and proportionate. The Home Office, Parliamentary Security Department and the Police work closely to both assess the threat posed to Parliamentarians and provide security measures for them in Westminster and in their constituencies – these measures are kept under continuous review.

Whilst Parliamentary Security Department are responsible for the security of MPs, since the General Election the Home Office has also assumed responsibility for the provision of protective security for Government Ministers. Despite the significant protective security provision available to MPs and Ministers, often police struggle to get criminal justice outcomes as evidence is either not brought forward or is deleted by well-meaning staff who do not want to expose their principal to the horrific abuse that streams into inboxes.

The Government recognises the essential role that MPs play in their own security. We support the recommendation that MPs and their staff proactively engage with the Parliamentary Security Department (PSD) and

take advantage of available security measures to enhance their protection. The Government fully endorses the efforts of PSD in supporting this objective.

Recommendation 12 (para 80, report 1)

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.

Response:

The Security Minister was clear during his oral evidence session to the Speaker's Conference, and has been clear since, that harassment and intimidation must never become part and parcel of the role of an elected representative. Through the Defending Democracy Taskforce, Government has undertaken a range of work to challenge this perception.

This work includes but is not limited to the creation of new guidance, both for returning officers and for police, so they know what to expect when dealing with an elected representative who is a victim of a crime.

As noted by the Conference, it is important that as a system — across police, government and Parliament — we develop a better understanding of the nature and scale of harassment and intimidation experienced by elected representatives. This work must include an in-depth review into this activity to understand the motivations of perpetrators, as outlined in recommendation 21, and we will take this forward alongside the review of harassment and intimidation already underway.

The spirit of this recommendation is also met in legislative changes the Government is bringing in through the legislation announced by the Security Minister to restrict protest outside the homes of elected representatives.

Furthermore, in the Strategy for Modern and Secure Elections, the Government is clear that this is a serious issue and is taking concrete steps to improve the safety and security of candidates and elected representatives. In the Strategy, we announced the introduction of an aggravating factor for those who harass or intimidate elected representatives, candidates and electoral staff. This demonstrates Government's commitment to ensure that any criminal behaviour towards elected representatives is dealt with the most serious consequences.

Recommendation 13 (para 87, report 1)

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 14 (para 91, report 1)

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.

Response:

While this recommendation is for the police, who are operationally independent, Government welcomes the principle of greater proactivity when tackling intimidation against MPs and other elected representatives. Government remains supportive of the new approach which PLaiT is taking with its offender management approach.

Government will provide support in the development of any guidance the police agree to take forward, to ensure it works hand-in-hand with the guidance already being developed by Government for police and returning officers. Government continues to stand ready to work with the Devolved Governments regarding the introduction or development of any prospective guidance.

Where there are other areas that guidance could prove beneficial, the DDTF will coordinate work across relevant government departments and the police to ensure that it is as effective as possible. Such guidance could include the recommended clarification of criminal thresholds.

Public attitudes

Recommendation 17 (para 30, report 2)

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 18 (para 33, report 2)

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.

Recommendation 19 (para 34, report 2)

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 20 (para 35, report 2)

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.

Response

The Government accepts the committee's view of the importance of strengthening citizenship education. The Government also recognises the role that citizenship education can play in supporting young people to understand how to engage positively with politicians and the political system and that this is fundamental to the successful implementation of the Government's manifesto commitment to extend the right to vote to 16- and 17-year-olds.

The Curriculum Review's report and the Government's response have now been published. We welcome the Review's recommendations and have committed to looking for the earliest opportunity to make citizenship a new requirement for key stages 1 and 2 – focused on the most essential content. This includes democracy and government, as well as media literacy, law and rights, financial literacy, and climate education. We have committed to refreshing the programmes of study for each curriculum subject in line with the Review's recommendations and publish a revised national curriculum in 2027 for first teaching in 2028.

The secondary citizenship curriculum will build on primary content and fit with the content in other subjects to ensure that all pupils get an essential grounding in a range of topics which include democracy, government and

law. We are committed to ensuring that democracy education reinforces the importance and value of participating positively in our democracy, and inspires greater democratic involvement, starting at sixteen and continuing into adulthood, by equipping pupils with the relevant knowledge and understanding. We believe that improved citizenship education, combined with a lower voting age, will allow the first experience young people have with our democratic system to lead to a lifelong habit of informed, engaged, and responsible participation.

DfE is already working with MHCLG on supporting democratic engagement and will work with the Parliament Engagement and Education team on how they can support citizenship education in schools in line with the recommendations.

Whilst recommendations 18, 19 and 20 are not for the Government to respond to or implement, we champion and encourage all public office holders to proactively engage with schools and students to enhance political engagement and positive democratic participation.

Recommendation 21 (para 44, report 2)

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 21 (para 45, report 2)

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.

Response:

The Government works closely with PLait in reviewing incidents that happen across force areas that are fed back through from the Op BRIDGER SpOcs across the country. This provides a basis for data collection and analysis at a basic level to help develop our understanding of trends where MPs are victims of crime and related incidents. However, Government has acknowledged that the evidence base needs to be further developed to provide a greater understanding of the perpetrators of these crimes. A deeper understanding of those who engage in abusive activity directed at politicians and their motivations is required to establish the most effective ways of reaching perpetrators.

The Home Office, under the Defending Democracy Taskforce is reviewing this activity, working with police, Parliamentary authorities and the Electoral Commission. We need to better understand trends, motivations and methodologies and a more detailed picture of victims to most effectively update our response to harassment and intimidation during election periods and outside of them. This includes identifying gaps and vulnerabilities and developing recommendations to strengthen the response, as well as a clear delineation of online versus in-person activity and its impact. This work will report to the Taskforce. The issue is complex, and it is important that we get it right.

While the Government recognises the importance of raising public awareness about the unacceptability of abuse and intimidation directed at elected representatives and is committed to taking robust action to deter such behaviour, including through communications, it does not accept recommendation 21.

Across Government, Parliament and police we need to develop a more comprehensive understanding of the evidence of the scale and prevalence of abuse as well as the motives and perpetrators before determining the most effective approach for a targeted campaign. This will allow us to better target appropriate communication campaigns going forward. We are mindful of the risk that a widespread public awareness campaign akin

to a public health campaign could inadvertently amplify the issue among the wider public or embolden those who may be inclined to engage in harassment of elected representatives.

Similarly to the evidence provided by Professor Ramanna to the Conference, the Government views that those individuals most likely to perpetrate abuse are unlikely to be receptive to government-led messaging, particularly when delivered through broad public campaigns.

The Government and the Electoral Commission have already begun delivering communications activity, proactively highlighting support for candidates ahead of next year's local elections, emphasising that any abusive behaviour will not be tolerated, and highlighting the powers police have. The Government announced to the media the introduction of legislative amendments earlier this month to restrict protests outside public office holders' homes and highlighted the penalties that those guilty of such a future offence would face.

The Government will continue to seek out opportunities to carry out communications activity through the media and stakeholder channels to highlight the work of the Defending Democracy Taskforce to counter this abusive behaviour. We are also working closely with partners such as the Electoral Commission, the Local Government Association, and law enforcement to support and amplify deterrence messaging, and to publicise the penalties imposed on those convicted of such offences. Ahead of the local election campaigning period next year, we will plan further communications and media activity, to highlight support for candidates and to highlight the consequences for engaging in abusive behaviour, and this will include exploring the possibility of a cross-party communications moment to show unity on this issue and help maximise receptiveness.

The Government will continue to monitor the impact of this approach and emerging insight and research into the scale of the issue and continue to review the effectiveness of our messaging.

Recommendation 22 (para 55, report 2)

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

Recommendation 23 (para 59, report 2)

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).

Recommendation 24 (para 71, report 2)

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 25 (para 75, report 2)

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.

Response:

As the media is independent from the Government, these recommendations are for IPSO, Impress and Ofcom to respond to. The Government does not intervene in or oversee the work of the press, including the working methods of journalists, publishers and the independent press regulators. A free, strong and plural media plays an essential role in democracy. It is a key source of trustworthy information and plays a vital role in holding those in power and public institutions to account.

Whilst our commitment to this freedom is unshakeable, the press has a responsibility to set and adhere to high ethical and professional standards and must also operate within the bounds of the law. We are clear that these high standards must include taking steps to ensure that misleading, inaccurate or distorted information is not published and providing access to clear, timely and effective routes to redress when these high standards are not met.

To uphold these high standards, and to support media plurality, there are different regulatory systems in place for broadcast and newspapers, reflecting the varied ways people consume different forms of media. While

accuracy in reporting is vital for all forms of media, the public can choose TV and radio for impartial news, while the press can offer a broad range of different perspectives and arguments, as they are free to editorialise and campaign, and are not required to uphold the same standards of due impartiality.

Broadcasters are regulated through Ofcom's Broadcasting Code, which includes rules that prohibit material which is likely to encourage or incite crime or lead to disorder. Broadcasters must also avoid unjust or unfair treatment of individuals.

Doorstepping as a practice is not prohibited under Ofcom's Broadcasting Code, though current guidance states that it should not normally take place unless a request for an interview has been refused or it has not been possible to request an interview, or there is good reason to believe that an investigation will be frustrated if the subject is approached openly.

As for the press, it is self-regulated. Within this system, the majority of traditional publishers are members of the Independent Press Standards Organisation (IPSO), many others are members of the Independent Monitor of the Press (Impress), and several more, including the Financial Times and the Guardian, have chosen to stay outside both these regulators with their own detailed self-regulatory arrangements.

It is the role of these independent regulators to set codes of conduct and these provide guidelines on a range of areas for the publishers they regulate. The most relevant of these in relation to the concerns set out in the Speaker's Conference Second Report are accuracy, privacy and harassment. These codes are available on the regulators' respective websites. If they find that a publisher has broken their code of conduct, regulators can order corrections. IPSO can also order critical adjudications and Impress can levy fines.

To ensure these standards remain relevant in an ever-changing media landscape each regulator has a different process for updating and enforcing the codes. For example, the IPSO editors' code of practice is independently written and reviewed by the Editors' Code Committee. The latest version came into effect in January 2025. It is the responsibility of editors and publishers to apply the Code to editorial material in both printed and online versions of their publications. The Impress Code Committee led a two-year review between 2020 and 2022 to update their Standards Code, which consisted of a call for evidence, workshops, research and a public consultation.

To maintain the independence of this system from the Government, we do not interfere in the work or operational decisions of press regulators and neither do we arbitrate on the content of press regulators' standards codes,

or the application of the public interest test. The independent regulators are solely responsible for this activity, including their activity to update and maintain their standards codes.

Similarly, Ofcom, as the independent regulator for broadcasting, is responsible for drafting and enforcing the Broadcasting Code and associated guidance. The Government does not intervene in Ofcom's operational decisions or its regulatory duties.

No one should ever face abuse, intimidating commentary or threats to them personally and we agree when mistakes are made by people in public office they should be held to account through appropriate democratic and legal means.

Looking ahead, the Government has been clear that we want to ensure the balance is right between accountability and press freedom, which is essential to ensure the public has access to trustworthy information from a range of sources. We are therefore carefully considering next steps to determine the best route forward to ensure public trust and accountability, in our news media.

The Criminal Justice Response

Recommendation 26 (para 96, report 2)

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 antidemocratic) 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 27 (para 97, report 2)

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 28 (para 106, report 2)

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 29 (para 112, report 2)

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.

Response:

The coordination of the police response to these issues is a matter for the police to respond to, however the Government's view is that anyone who breaks the law and harasses a candidate or elected representative should face the full force of the law. The Security Minister wrote to Chief Constables reminding them of the powers they have available to them and encouraging them to use them ahead of the May election. The police have acknowledged that during the general election, there were issues with consistency of their approach.

Recommendation 30 (Para 114, report 2)

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.

Response:

Police are building an Op Ford Threat Assessment Centre to pull together intelligence and crime data for offences committed against locally elected representatives. When fully operational, this will use the same platform as crime and intelligence reporting for MPs, making data collection and analysis much more efficient and in line with our overall ambition for threat reduction. It will also enable operational partners act upstream and track individuals in the system across both MPs and locally elected representative cohort.

The Government partly accepts recommendation 30. We recognise the importance of reliable data in assessing the threats faced by elected officials and candidates for public office. However, the CPS does not collect official statistics in this area. CPS management information is available only for cases referred for a charging decision. This data is compiled manually and relies on prosecutors notifying the central team when a case involves an elected official.

In light of these limitations, we do not consider CPS management information to be a reliable tool for addressing this issue. We will consider whether there may be other more appropriate avenues to develop data streams, and consider whether any new products need to be introduced to meet this need.

The DDTF covers a range of issues. Ministerial attendance from the Ministry of Justice will be an important future part of the joined-up approach to tackling harassment and intimidation being driven the DDTF. Therefore, a relevant MoJ Minister will be invited to attend the Taskforce when the focus is on strategic and deep dive discussions on responding to harassment and intimidation. This will mean the criminal justice system's response will be part of the programme of work to better protect those working in our democracy.

Recommendation 31 (para 120, report 2)

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 32 (121 , report 2)

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 33 (122, report 2)

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.

Response:

In response to recommendation 31, responsibility for implementation of the measure sits with the independent Sentencing Council and its devolved equivalents. That being said, Government will engage with them regarding the issuing of guidance on protective orders in cases where MPs or their staff are targeted.

We will continue to work with the police on technological developments, though the implementation of any new tactics is for them. Recommendation 33 is for Parliament to answer.

Recommendation 34 (para 125, report 2)

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.

Response:

The Government recognises the importance of resolving these cases as quickly as possible.

Mechanisms already exist to enable charging decisions for this type of offending to be prioritised during election periods. Chief Crown Prosecutors and Chief Constables can agree to prioritise the charging of certain categories of offending where appropriate, taking into account competing pressures and priorities within the criminal justice system.

Before significant election periods, CPS can remind Chief Crown Prosecutors of this mechanism so they can discuss it with Chief Constables, ensuring police partners are aware that this option is available if concerning offending trends are identified during an election period.

However, the CPS has no control over the length of an investigation (which is a matter for the police), nor over the time from charge to first appearance or the timetable for listing a case for trial (both of which are matters for the independent judiciary).

The criminal courts can and do expedite the treatment of certain cases and categories of cases in appropriate circumstances. Most MP related cases are already subject to special consideration as part of the Special Jurisdiction of the Senior District Judge (Magistrates' Courts) and Chief Magistrate in accordance with paragraph 5.14.6 in Criminal Practice Directions - *offences involving royalty or Parliament*. These cases are then flagged to the Crown Court if sent for trial or committed for sentence.

Decisions on managing, prioritising and listing cases before the courts are a matter for the independent judiciary. However, as previously indicated, the timely completion of any criminal case through the courts will necessarily be dependent on a range of factors, not limited simply to the nature of the alleged offence concerned. Additional factors will include the evidence available and presented (including its volume and complexity), the plea (and its timing) of the defendant, and any requirements for additional assistance (specialist reports etc) ahead of any required sentencing decisions.

For the above reasons agreeing specific targets for this cohort of cases is therefore problematic but given the specialised handling of these cases, magistrate court or Crown Court judges would almost certainly consider requests to expedite them. Provided that the police investigation has completed to the requisite quality standards and in good time for a charging decision to be made, and the prosecution flag to the court the public interest and need for expediting a case - for example by making representations that the case should be heard within an election period - this can be taken into account when making a decision on prioritisation and listing.

Recommendation 35 (para 133, report 2)

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 36 (para 136, report 2)

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 37 (para 137, report 2)

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.

Response:

The Government has announced a commitment to introduce a new statutory aggravating factor for offences motivated by hostility towards candidates and will legislate to do so at the earliest opportunity.

As is the case for disqualification orders, the aggravating factor will cover offences which are motivated by hostility towards a member of one of these groups, rather than requiring the offence having been committed against them.

This ensures that the aggravating factor captures incidents such as those described by the Conference, for example offences targeting an MP’s staff. Empowering courts to increase sentences for offences where such hostility is present will underline the severity of the offence and ensure harsher sentences can be imposed against such offenders.

The Government recognises that abuse and intimidation of MPs and candidates has disproportionately targeted those who are underrepresented in politics, including women and those from minority ethnic backgrounds. As the former Policing Minister set out while providing evidence to the Speaker’s Conference, the Government is reviewing the recommendations from the Law Commission report.

Recommendation 39 (para 161, report 2)

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 40 (para 162, report 2)

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.

Response:

The Government recognises the seriousness of threats directed at MPs, candidates, and other public figures, and share the Committee’s concern about ensuring these are dealt with effectively. Social media platforms have a responsibility and must all step up to address these harms. To support this, the Government routinely engages with all major social media platforms, including during election periods, on risks posed to the UK and its citizens, and to ensure the protection of UK democratic processes.

The Government agrees that MPs and candidates should be supported in making use of the protective tools available to them and feel empowered to leave platforms judged to present higher risks than benefit to their work, and believes that political parties, MPs, and candidates are best placed to implement these recommendations.

The Government remains committed to tackling online harms, including through the ongoing implementation of the Online Safety Act which places duties, which are now in effect, on social media platforms to remove illegal content.

Under the Act, Category 1 services will also be required to offer user empowerment features which, if applied, will enable adults to choose whether or not to engage with content including that which is abusive, or incites hate, on the basis of race, religion, sex, sexual orientation, gender reassignment or disability. When applied, these features will reduce the likelihood that adult users of these services are exposed to certain categories of content or will alert them to the nature of it. Adult users will also be able to control their exposure to non-verified users, meaning users who choose not to take up the option to verify their identity, which Category 1 services are required to offer under the Act. Ofcom are due to consult on these user empowerment tools in 2026 after it establishes the register of categorised services.

The Government welcomes the Conference's agreement that these tools will play an important part in protecting candidates from needing to see or engage with abusive content online.

Recommendation 41 (173, report 2)

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, antispam 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 42 (174, report 2)

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.

Response:

The Government welcomes and supports in spirit the recommendations for the Parliamentary Digital Service and MPs to improve and utilise available email protection systems.

Whilst the implementation of these recommendations falls within the remit of Parliament, we appreciate the proactive approach suggested to explore automated prompts, alternative contact systems and increasing awareness of existing screening facilities.

Recommendation 43 (190, report 2)

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 USUK 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.

Response:

The Government's position is clear - political intimidation and abuse of those participating in public life, whether as voter or as an elected representative, is completely unacceptable and should be subject to the same threshold for platform action as other types of threats or abuse.

The Online Safety Act requires providers to treat content as illegal where there are reasonable grounds to infer its illegality, based on all relevant and available information. This obligation applies equally, regardless of who the target of any illegal content is. Platforms must not have fewer protections

in place for a public figure than any other UK user when it comes to illegal content. Providers must have systems in place to remove this content when it meets the illegal threshold.

Furthermore, under the Act's illegal content safety duties, providers are required to proactively assess, mitigate, and manage risks of illegal content, including through safety-by-design measures. Ofcom will review whether providers' systems and processes - whether automated or human - are consistent with these statutory duties.

The Act includes important safeguards to protect users' rights, particularly freedom of expression. Providers must take these rights into account when designing and operating their safety systems. For the largest social media platforms, this includes paying special attention to the importance of certain types of content, such as journalism and content of democratic importance, when making moderation decisions. Political speech also benefits from enhanced protection under Article 10 of the European Convention on Human Rights.

Ofcom, as the independent regulator, sets out in its codes of practice the steps providers can take to meet these duties. In some cases, this may mean certain platforms introduce additional measures in their moderation processes to ensure that political and journalism-related content is treated appropriately. However, these duties do not override the requirement to remove content that amounts to a criminal offence, regardless of who the victim is. Providers must strike a careful balance—removing illegal content while safeguarding lawful political expression.

While the Online Safety Act does not impact what legal content adult users are able to access on a platform, the Act empowers adult users to have more control over their online experience. For example, the largest services (known as 'Category 1' services under the Act) will have extra duties related to protecting all people from abuse, including elected representatives. These services will have to have systems and processes in place to consistently remove content that is prohibited in their terms of service. Where providers say they will remove certain kinds of content, such as abuse towards elected representatives, they will need to fulfil these commitments consistently. As a result, users will be able to trust that any commitments made in terms of service will be upheld, empowering them to make informed decisions about which platforms they choose to use.

Platforms will also need to put in place user empowerment and user verification tools for adult users, enabling these users to have greater control over their online experience. This may include offering prompts or stronger default settings. In 2026, Ofcom will consult on these additional duties including those relating to terms of service, user empowerment, user verification, and protections for content of democratic

importance. As with other areas of the Act, Ofcom has strong enforcement powers should they find that platforms are not complying with these duties. Companies can be fined up to £18 million or 10% of their qualifying worldwide revenue, whichever is greater.

As set out in the Secretary of State for Science, Innovation and Technology letter to Ofcom on 12 November 2025,¹ Ofcom needs to maintain an urgent sense of momentum to implement the remaining duties and ensure that we are maximising the levers that the Act provides. The Government agrees that it is important to monitor how these duties work in practice, and we will do so before considering further steps. We remain committed to taking further action if evidence shows that more is needed.

Ahead of local and devolved elections in May 2026, we will engage with the major social media platforms on their user safety responsibilities and the need to address harassment and intimidation of politicians and candidates.

The UK-US Data Access Agreement is a critical tool for UK law enforcement and intelligence agencies. The Agreement ensures that UK authorities can submit requests for the content of communications directly to communications service providers, including social media platforms and messaging services, located in the United States. The Agreement has allowed our agencies access to more data, more quickly than ever before to support the prevention, detection, investigation and prosecution of serious crime. Serious crime is defined under the Agreement as an offence that is punishable by a maximum term of imprisonment of at least three years. The Agreement has been transformative for law enforcement and the Home Office will continue to work closely with operational partners over the coming years to maximise the benefits that the Agreement provides.

Recommendation 44 (191, report 2)

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.

¹ [Implementation and enforcement of the Online Safety Act: follow up letter from DSIT Secretary of State to Ofcom - GOV.UK](#)

Response:

The Online Safety Act provides Ofcom with extensive information-gathering powers to scrutinise the operation of recommendation algorithms. These includes requiring platforms to demonstrate the real-time operation of their algorithms and to conduct practical tests to observe them in practice.

Ofcom can also require a report from a skilled person, such as a researcher, into a failure, a possible failure, or a risk of a failure by a provider of a regulated service to comply with duties in the Act, for example, algorithms promoting illegal content.

Ofcom can also require categorised services to include information about their algorithms in their annual transparency report, including the role algorithms play in the display, promotion, restriction, discovery or recommendation of regulated content.

The Government recognises that online harms data is only directly available at the discretion of tech companies, and researchers have cited technical and procedural barriers which prevent high-quality research.

We agree that transparency and a robust evidence base is critical. This is why the Government legislated in the Data (Use and Access) Act to give the Secretary of State the power to create a regulatory framework to allow researchers to access online safety data, placing research on a firm statutory footing.

Ofcom published a report on exploring researchers' existing access to data, the barriers to access, and how greater access might be achieved in June 2025. The Government is carefully considering that report and will consult on the framework in due course.

Recommendation 45 (200, report 2)

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.**

Response:

The Government recognises the value of parliamentary scrutiny and the expertise that parliamentarians in both Houses provide and is committed to working with Parliament to ensure that select committees have the information they need, including providing advance notification to select committees where possible and appropriate, in line with the commitments made to the Chairs of the Science, Innovation and Technology and Communications and Digital Committee in the letter of 6 June

Ofcom, as an independent regulator is accountable directly to Parliament for its work but Government supports Ofcom working closely with select committees to support effective scrutiny.

In terms of future revisions to the Act, the Government is required to conduct a Post Implementation Review of the Online Safety Act, which will be laid before Parliament. The review will assess the performance of the legislation against its primary objectives, including how the online safety regime has protected children from harmful and illegal content on regulated services. The Government and Ofcom have developed a framework to monitor the implementation of the Online Safety Act and to evaluate the core outcomes to ensure any future revisions of the Act are evidence based.

Recommendation 46 (204, report 2)

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 48 (206, report 2)

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.

Response:

The Government recognises the serious impact of online abuse and intimidation targeted at MPs and candidates during elections and agrees that platforms must step up and take robust action to protect them.

While the Online Safety Act provides one of the strongest online safety frameworks anywhere in the world, including providing protections against illegal content, such as illegal harassment, intimidation and abuse, we must ensure that protections keep pace with evolving threats, including to UK democracy. The Government will continue to actively review the framework – this will include meeting with and hearing from stakeholders including MPs and candidates to understand where the Act can be strengthened through evidence-based measures. The Government also supports Ofcom in continuing to iterate and develop codes under the existing framework as both harms and the evidence base continues to evolve.

Recommendation 47 (205, report 2)

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.

Response:

The Government's position is clear - political intimidation and abuse of those participating in public life, whether as voter or as an elected representative, is completely unacceptable and should be subject to the same threshold for platform action as other types of threats or abuse.

While the Online Safety Act does not impact what legal content adult users are able to access on a platform, the Act empowers adult users to have more control over their online experience. For example, the largest services (known as 'Category 1' services under the Act) will have extra duties related to protecting all people from abuse, including elected representatives. These services will have to have systems and processes in place to consistently remove content that is prohibited in their terms of service. Where providers say they will remove certain kinds of content, such as abuse towards elected representatives, they will need to fulfil these commitments consistently. As a result, users will be able to trust that any commitments made in terms of service will be upheld, empowering them to make informed decisions about which platforms they choose to use.

Platforms will also need to put in place user empowerment and user verification tools for adult users, enabling these users to have greater control over their online experience. This may include offering prompts or stronger default settings. In 2026, Ofcom will consult on these additional duties including those relating to terms of service, user empowerment, user verification, and protections for content of democratic importance. As with other areas of the Act, Ofcom has strong enforcement powers should they find that platforms are not complying with these duties. Companies can be fined up to £18 million or 10% of their qualifying worldwide revenue, whichever is greater.

As set out in the Secretary of State for Science, Innovation and Technology letter to Ofcom on 12 November 2025,² Ofcom needs to maintain an urgent sense of momentum to implement these remaining duties and ensure that we are maximising the levers that the Act provides.

Recommendation 49 (207, report 2)

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.

2 [Implementation and enforcement of the Online Safety Act: follow up letter from DSIT Secretary of State to Ofcom - GOV.UK](#)

Response:

The Government supports Ofcom as it continues to implement this vital regime. Ofcom has built a multidisciplinary team with expertise drawn from regulation, technology platforms, law enforcement, civil society, and academia. 2023/24 figures show that Ofcom had 452 staff working on online safety across the organisation. This is in line with the National Audit Office's Preparedness for online safety regulation report.

Following an extensive business case process, the Government agreed a multi-year funding settlement for Ofcom's online safety work from 2025/26 - 2027/28. This has provided certainty for Ofcom and enables it to forward plan its regulatory activity. The Government remains committed to reviewing this settlement regularly with HM Treasury and Ofcom to ensure it remains fit for purpose, particularly as the regime matures and new challenges evolve.

Recommendation 50 (213, report 2)

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.

Response:

This Government shares the conference's concern about the impact of mis- and disinformation, including the role of deepfakes, on candidates, MPs, and UK elections and is committed to addressing it.

The Act requires in-scope services to assess and mitigate risks from illegal content, including AI-generated deepfakes that amount to an offence under section 106 of the Representation of the People Act or the false communications offence. Ofcom's Codes of Practice set out measures in

areas such as risk management, user reporting, and content moderation. Providers are expected to implement effective processes to monitor and remove such content.

We can confirm that we will be monitoring the implementation and impact of the false communications offence as part of ongoing work. Government is also carefully considering the need for any updates to existing electoral offences to explicitly capture deepfakes.

The Government are also strongly committed to addressing non-consensual sexual deepfakes and intimate image abuse. The sharing of, or threatening to share, a deepfake intimate image without consent is a criminal offence under the Online Safety Act. The Government continues to act against this abhorrent harm and has strengthened the Act to make the intimate image abuse offences priority offences, requiring in-scope services to prevent such content from appearing online in the first place and swiftly removing it if it does.

More broadly, the Government made a manifesto commitment to ban the non-consensual creation of sexually explicit deepfake images and we have legislated to honour that commitment in the Data (Use and Access) Act, ensuring that offenders face the appropriate punishments for this awful harm.

Going further still, the Government has announced its intention to legislate to ban ‘nudification’ tools that use AI to turn normal images of real people into fake nude pictures and videos without their consent. This new criminal offence will make it illegal for companies to supply tools designed to create non-consensual intimate images, targeting the problem at its source.

Recommendation 51 (217, report 2)

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.

Response:

The Government agrees that significant distress is caused by doxing and pile-on harassment. Existing legislation already provides a range of protections for individuals subjected to such behaviour, and the Online Safety Act strengthens these protections for online users.

In relation to pile-on harassment, where multiple individuals collectively target a single person, typically online, through abusive messages, ridicule, or the sharing of private information, a range of criminal offences may apply depending on the circumstances. Such behaviour may amount to

harassment under the Protection from Harassment Act 1997, which applies equally to online and offline conduct. This includes offences where a person pursues a course of conduct which they know, or ought to know, amounts to harassment, under sections 2 or 4, as well as stalking offences under sections 2A and 4A. The 1997 Act also allows for liability where groups act in a coordinated manner, including under section 1(1A).

Where behaviour amounts to harassment under the Protection from Harassment Act 1997, it is a priority offence under the Online Safety Act. Priority offences under the Online Safety Act reflect the most serious and prevalent illegal content and activity. In practice, this means companies must take proactive measures to prevent and remove any such content from appearing on their platforms. In addition, the Online Safety Act introduced false and threatening communications offences, which could capture similar behaviour.

The false communications offence makes it illegal for an individual to send information they know to be false intending to cause harm. The threatening communications offence captures communications conveying a threat of death, serious injury, rape and serious financial harm. Other criminal offences may also apply, including under the Malicious Communications Act 1988 and section 127 of the Communications Act 2003.

To ensure the criminal law continues to provide the clearest possible framework for identification, management and prosecution of stalking behaviours, Richard Wright KC has been appointed to conduct an independent review of stalking legislation. The review covers the stalking and harassment offences in the Protection from Harassment Act 1997, and where relevant, will also consider related offences such as coercive and malicious communications. The full review, including any recommendations, will be submitted to the Home Secretary by the end of March 2026.

Beyond criminal law, further protections against doxing and pile-on harassment will be introduced as the additional duties for categorised services are implemented. Where doxing or pile-on harassment is banned in the terms of service for a Category 1 service (the largest services), such services are required to apply these terms consistently and transparently, and have systems in place to remove such content. The Online Safety Act requires Category 1 services to have clear and accessible Terms of Service, setting out what kinds of legal content for adults they don't accept on their platforms.

The Act also tackles online abuse from anonymous users. As stated previously, where anonymous abuse does not amount to an offence, adult users of the largest services will have the choice to filter out content from non-verified users. If applied, these features will enable adult users of the

largest services to reduce the likelihood that they see content from non-verified users and prevent non-verified users from interacting with their content.

Ofcom's recently published [guidance](#) for how tech companies can improve women and girls' safety online specifically addresses pile-on and co-ordinated harassment. The guidance makes it clear what platforms should already be doing under existing legislation to benefit all users. It also suggests additional steps services can take, including imposing rate limits to prevent mass-posting in pile-on scenarios, and adding fact-checking and labelling to content.

Appendix 2: Letter from Gavin Stephens QPM, Chair of the National Police Chiefs’ Council and Jon Savell, DAC Specialist Operations, 15 January 2026

We are writing following the publication of the second report of the Speaker’s Conference on the security of candidates, MPs and elections, published on 27 October 2025. The findings of this report, building upon the first phase of the Conference, emphasise the scale of abuse, intimidation and threat facing candidates and MPs across the UK.

Evidence submitted to the Conference and published by the Electoral Commission and academic partners confirms the severity of the issue; for example, over half of candidates in the 2024 General Election avoided campaign activity due to fear of abuse, and up to 85% reported harassment, abuse or intimidation during recent election cycles, particularly women and candidates from minority backgrounds.

It is clear that policing, government and partners must respond with an approach that is consistent, preventative, intelligence led and sensitive to the democratic context. Below we outline the existing structures that support elected officials, followed by responses to each recommendation.

Existing Structures Supporting the Security of MPs and Candidates

Operation Bridger

Operation Bridger provides UK policing’s operational framework for supporting the safety and security of MPs when away from the Parliamentary Estate. Established after the murder of Jo Cox MP in 2016

and strengthened following the murder of Sir David Amess MP in 2021, it coordinates Single Points of Contact (SPOCs) across all forces and works closely with the Parliamentary Liaison and Investigation Team (PLaIT). It is underpinned by national guidance and minimum standards to ensure consistency across 43 forces.

Defending Democracy Task Force & Operation Ford

In February 2024, the Defending Democracy Task Force introduced the Defending Democracy Policing Protocol, expanding Bridger-style protections to other elected officials through

Operation Ford. Each force now has a funded Force Elected Official Adviser (FEOA), enhancing advice, threat assessment and local coordination.

Both Bridger and Ford have been tested during the 2024 General Election and 2025 local elections, offering strong learning on threat patterns, demand, and inter-agency coordination.

NPCC Elections Portfolio

The NPCC Elections Portfolio leads on electoral offences under the Representation of the People Act and works closely with the Electoral Commission and the City of London's Economic and Cyber Crime Academy. It routinely shares data with the Bridger Network, particularly during election periods, recognising the overlap between electoral offences, hate crime and targeted abuse.

Responses to recommendations

Recommendation

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.

Response

National coordination for police intelligence and planning during election periods policing is delivered through the National Police Coordination Centre (NPoCC), which oversaw the 2024 General Election and will again support the forthcoming local elections. A Gold, Silver, Bronze (GSB) command structure will be recommend to affected forces and the College of Policing (CoP) standardised planning templates will be utilised to ensure consistent and risk-assessed approaches across all 43 forces.

The integration of planning with returning officers, the Electoral Commission, and Joint Election Security Planning (JESP) partners ensures local insight is built into national consistency. SPOCs from Bridger, Ford and Elections portfolios will continue to contribute collectively, recognising the complementary nature of their roles.

The application of this coordinated model during local elections will provide a strong operational testbed ahead of the next general election.

Recommendation

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.

Response

Work is already underway, led by the College of Policing with contributions from the Home Office, CPS, NPCC portfolios, and PLaiT. This guidance will integrate thresholds across harassment, malicious communications, public order, and electoral offences, recognising that some offences arise uniquely during election periods.

To ensure accessibility, policing will develop:

- Operational guidance for officers and returning officers
- Specialist modules for SPOCs

- A simplified, user-friendly version for MPs, candidates and staff to clarify when and how to report concerns

This addresses the Conference's finding that candidates often lack clarity about thresholds and expectations, which has historically contributed to only 9% of candidates reporting incidents to police during recent elections.

Recommendation

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.

Response

The Conference's findings, supported by recent case law and the experiences of MPs such as Alex Jones, outline a review of this areas is required.

Work is ongoing at both strategic and operational levels:

- The Lord McDonald Review is examining practical mechanisms for earlier intervention
- MSAFE, PLaiT, and the College of Policing are shaping guidance on proportional interventions, including use of anti-social behaviour legislation
- Frontline awareness training will emphasise earlier, intelligence led action to prevent escalation

An assertive approach to harassment especially online combined with SPOC led support to remove harmful content is vital, particularly given the Speaker's evidence that online normalisation of abuse emboldens perpetrators.

Recommendation

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.

Response

Compliance with the Victims' Code is mandatory, and PLaiT already models best practice by providing consistent, scheduled updates to MPs.

To enhance national consistency, we will:

- Work with NPCC and the College of Policing to standardise update protocols
- Ensure SPOCs confirm with each MP or candidate their preferred method and frequency of updates
- Address communication gaps by outlining approved communication tools aligned with NPCC digital guidance

Ensuring transparency builds trust and mitigates the sense of isolation frequently reported by MPs and candidates experiencing abuse.

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.

Response

Centralised oversight to improve consistency while maintaining essential local operational responsibility is supported. It is proposed this is achieved through an NPCC led portfolio, headed by a Chief Officer, to:

- Coordinate intelligence, investigations, and standards

- Integrate specialist expertise across Bridger, Ford, Elections and digital threat portfolios
- Ensure local forces retain responsibility for site-based protective security and community relationships
- Prioritise the national response to anti-democratic crimes
- Ensure clarity around crime categorisation and thresholds
- Provide specialist support to local forces while preserving local ownership

This approach mirrors successful NPCC governance structures and avoids the cost and complexity of standing up a large central unit prematurely. The role profile for a national lead is being agreed with partners, prior to advertisement.

NPCC Elections and related portfolios support integrating their expertise into a broader Democracy Protection Portfolio, while retaining specialist SPOCs and overall lead given the technical nature of electoral offences.

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.

Response

We agree. A phased model led by the NPCC allows intelligence, coordination and standards to be enhanced quickly, while generating essential insight into the workload associated with Op Ford before committing to full integration.

Understanding Op Ford's demand is critical to avoiding unintended dilution of Op Bridger resources, and it will be ensured resourcing assessments and cost modelling are completed before any structural merging.

Recommendation

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.

Response

Work is already under way with the Home Office and College of Policing on guidance covering investigative standards, crime recording and threshold clarity. Recent protest-related incidents have demonstrated the value of effective Counter Terrorism Policing liaison, and this relationship will continue to be strengthened.

Guidance on when threats should be considered for CT referral will be expanded, acknowledging the particular context of Northern Ireland, where historical and contemporary risks differ significantly.

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.

Response

Integrating electoral law policing into a wider anti-democratic crimes structure is logical and would improve resilience, consistency, and intelligence-sharing.

At present, collaboration between Election SPOCs and Bridger/Ford SPOCs is already well-established strategically. Tactical collaboration within forces will be strengthened through:

- Joint briefings
- Shared learning
- Resilience arrangements between the networks

This preserves specialist expertise while improving integration and situational awareness.

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.

Response

The exploration of new technologies, similar to those being developed for domestic abuse protection order enforcement, that could support the monitoring of restraining orders, stalking protection orders and other court-imposed restrictions involving MPs is supported.

Policing already ensures that MPs and candidates are informed of key developments such as:

- The imposition or expiration of protective orders
- Changes in offender behaviour or risk level
- Prison release dates or licence conditions

Enhancing technology supported monitoring will improve both enforcement and victim confidence.

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

Response

It is fully recognised female candidates face heightened risks. Research submitted to the Conference and by the Electoral Commission shows that:

- Women are disproportionately targeted with misogynistic abuse
- Female candidates report avoiding certain campaign activities at significantly higher rates
- Online harassment is both more frequent and more personalised for women candidates

Policing plans will therefore explicitly consider gender-based risk factors, ensuring:

- Risk assessments reflect differentiated threat profiles
- SPOCs receive training specifically on gendered political violence
- Intelligence products include gender-specific indicators

- Local threat mitigation accounts for online abuse patterns directed at women

This aligns with the Speaker's Conference findings and ensures equal access to the democratic process.

Conclusion

The Speaker's Conference's detailed examination of the escalating threats facing MPs, candidates and the democratic process is welcomed. Policing remains committed to a preventative, intelligence led, trauma informed and nationally consistent approach. The measures outlined, combined with strengthened inter-agency collaboration, improved guidance, and the establishment of an NPCC led Democracy Protection Portfolio, will help ensure elected representatives can serve without fear and that democracy is safeguarded.

CC Gavin Stephens QPM

Chair of the National Police Chiefs' Council

Jon Savell

DAC Specialist Operations

Appendix 3: Letter from Alison Giles CB, Director of Security for Parliament, 5 December 2025

I am writing to you following the publication of the second and final report of the recent Speaker's Conference on the security of candidates, MPs and elections, published on 27 October 2025. As you know from our frequent dialogue on the topic, the Parliamentary Security Department (PSD) warmly welcomes the work the Conference has done to highlight areas where greater steps can be taken to ensure Members, candidates and elections can be made more secure.

We have already started implementing some of the recommendations; a detailed breakdown can be found below.

Recommendation

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.

PSD has a strong partnership with both the Home Office and Police, with both risk assessment and private security provision managed in partnership (with the Home Office now taking the lead for Government Ministers). This relationship underpinned an effective handover of security provision before the 2024 general election. The Government is in the process of drafting its response to the Speaker's Conference recommendations, but we have received assurance that they will work with PSD to ensure a smooth handover of these responsibilities when Parliament is dissolved ahead of the next election.

Recommendation

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.

PSD's Security Information and Risk Analysis Service (SIRAS) reviews the threat landscape regularly, maintaining connections with experts in government and the Police to ensure PSD's security arrangements are threat-led, dynamic and informed by up-to-date, authoritative information.

MPs' staff already benefit from several security measures, including those installed at Member's offices which ensure that they have a secure working environment. SOS Fobs are made available to staff, along with Situational Awareness Training. PSD also assess and respond to any exceptional, credible threats which are identified targeting MPs' staff.

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.

We are engaging with partners in the House to ensure the timely delivery of a visitor information system. There have been challenges in securing sufficient market interest in a standalone system so we are now looking at alternative mechanisms to capture visitors' identities in advance of their visit. PSD and Black Rod's Office already operates an effective process for banning visitors from the Estate based on an assessment of the risk they pose, although new visitor management strategies are likely to provide additional reassurance.

Alison Giles CB

Director of Security for Parliament

Appendix 4: Letter from Andy Smith, Managing Director and Chief Information Officer, Parliamentary Digital Service, 26 January 2026

We recognise the challenge outlined in the report and recommendations 51 and 52, which seek to address the volume and impact of abusive correspondence received by Members while preserving effective democratic engagement.

The Parliamentary Digital Service will explore how alternative approaches and technologies could help reduce the receipt of abusive email, and acknowledge that this is a complex area requiring careful consideration.

An iterative and exploratory approach will be adopted, where we learn by doing. This will enable us to gather feedback quickly on both the technology itself and the impact it has on correspondence between constituents and Members, and ensures we take a balanced approach that preserves the essential human aspect of this communication.

In support of this, we are already developing a small proof of concept to trial the use of contact forms with Members. We are grateful for the participation of a number of MPs who were part of the Speaker's Conference.

Importantly, any change in approach will require careful consultation with Members and guidance through appropriate political consensus and advice. We will keep the Administration Committee informed of progress on the pilot and the wider work in this area.

In line with the recommendations and alongside longer-term initiatives, we are examining near-term measures, including raising awareness of optional email filtering capabilities for Members and support staff, and determining the feasibility of implementing banner-style notifications on incoming emails that may contain abusive language.

Andy Smith

Managing Director, Parliamentary Digital Service and CIO

Appendix 5: Response from Parliamentary Education and Engagement Team

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.*

33a. The Education and Engagement Team has began work on the design of new resources for MPs when they meet schools independently. This will include a presentation slide deck they can use in the classroom with the option to play educational videos, and worksheets for students that teachers can print ahead of the visit that help the students focus on preparing to meet their MP. We will also update our guidance document on helpful information when visiting a school with support for MPs on safeguarding and photography. To begin with all resources will be digital and held centrally for MPs. Once this initial work is complete we will consult with Members about further resources they would find helpful when they visit schools.

33b. The Education and Engagement Team will extend the training and guidance on working with children that is currently offered to Members of the House of Lords via the Learn with the Lords education programme, We will pilot this work with smaller groups of both MPs and their office staff to begin with a view to launching an offer to coincide with the new MP classroom resources in 33a.

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.*

34 For UKPW 2026 all MPs will receive a list of all schools in their constituency signed up to participate in UK Parliament Week and all those who have not. This is with the intention that we can then work with MP offices to help facilitate visits. In order for MPs to have the opportunity to visit schools during Parliament we are reliant on the Friday of Parliament Week being available to MPs as a non-sitting day. We will support MPs with suggestions on how to use this Friday to meet their schools and with resources ready for their classroom visits.

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.*

35. The Parliamentary Education and Engagement Team will remain focused on being a Member focused service however we will expand our reach for UK Parliament Week to local government as a means to engage them with educational programming.

Appendix 6: Response from the Sentencing Council

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.

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.

Protective Orders

Currently, [comprehensive guidance on restraining orders](#) is included within the following relevant guidelines:

- [Common assault](#) – section 39 Criminal Justice Act 1988
- [ABH](#), section 47 Offences against the Person Act 1861
- [GBH](#), section 20 Offences against the Person Act 1861

- [Harassment and stalking](#), section 2 and section 2A Protection from Harassment Act 1997
- [Harassment \(fear of violence\)/ Stalking \(fear of violence or serious alarm or distress\)](#), section 4 and section 4A Protection from Harassment Act 1997
- [Threats to kill](#), section 16 Offences Against the Person Act 1861

A court may make a restraining order on conviction with or without an application from the prosecution, but, in practice, the prosecution would normally draw up a draft order and give the offender the opportunity to consider it. The order can contain only prohibitions and the prohibitions in the order must be:

- necessary to protect the person(s) to be protected from future conduct which either amounts to harassment of that person or will cause them to fear violence
- proportionate to that purpose, and
- clear and precise so that there is no doubt what the offender is prohibited from doing

Future Work

In response to these recommendations the Sentencing Council will, as part of its next round of miscellaneous amendments consider adding the guidance on restraining orders into the following guidelines:

- [Threatening behaviour – fear or provocation of violence](#), section 4 Public Order Act 1986
- [Disorderly behaviour with intent to cause harassment, alarm or distress](#), section 4A Public Order Act 1986
- [Disorderly behaviour](#), section 5 Public Order Act 1986

In addition, and again as part of our next round of miscellaneous amendments, the Sentencing Council will consider providing guidance on Disqualification orders under the Elections Act 2022. We note that the legislation states that where an adult offender is convicted of a relevant offence and that offence is aggravated by hostility relating to candidates for election or holders of public office, or an election campaigner the court **must** impose a disqualification order unless there are particular circumstances relating to the offence or to the offender which would make it unjust in all the circumstances to make the order. There is no requirement for an application to be made by the prosecution.

Any future guidance from the Sentencing Council on electoral disqualification orders would be subject to public consultation and would reflect the requirements as set out in legislation.

Letter from Lady Justice Juliet May, Chair of the Sentencing Council, 6 February 2026

Thank you for inviting the Sentencing Council to respond to your recent report. You have raised some further questions in your letter to me of the 4th February 2026 which I address below:

1. The Conference report noted specific concerns about how protective orders are imposed in cases where the victim is an MP or their staff. It therefore recommended that the Sentencing Council produce guidance specifically on protective orders in these cases. However, the Sentencing Council's response discusses providing guidance for particular offences not for particular victims. Can you clarify why this is?

The Sentencing Council was created by the Coroners and Justice Act 2009 to produce sentencing guidelines. The Act defines sentencing guidelines as follows:

120 Sentencing guidelines

(1) In this Chapter “sentencing guidelines” means guidelines relating to the sentencing of offenders.

(2) A sentencing guideline may be general in nature or limited to a particular offence, particular category of offence or particular category of offender.

The Council's guidelines and guidance follow these provisions and relate to specific offences or offenders. The way that judges and magistrates use sentencing guidelines in practice is by reference to the offence being sentenced.

The Council also has a statutory duty to have regard to ‘the impact of sentencing decisions on victims of offences’. The Sentencing Council's guidance on protective orders has this in mind. The guidance is applicable to all forms of victims and enables the courts to tailor the order to the specific case. Even in a case where the victim is an MP, there will be a wide variety of circumstances relating to the offender, the offence or behaviour and the victim that will be taken into consideration when preparing the

order. The current guidance on protective orders does not, therefore, propose specific factors for inclusion in an order but outlines the type of factors that may be appropriate depending on circumstances.

2. If the Council can only provide guidance on an offence-by-offence basis, would the introduction of a statutory aggravating factor for attacks on elected representatives allow the Council to produce specific guidance on protective orders that could be tied to crimes that were aggravated in this way?

When new statutory aggravating factors are created, the Council amends the relevant guidelines to ensure they reflect the legislation. Statutory aggravating factors make an offence more serious and will often result in an upward adjustment to the sentence. The Sentencing Council may choose to provide a more detailed explanation of the statutory aggravating factor (an expanded explanation) to assist the sentencer to determine whether the factor applies.

3. The Council has said it will “consider” providing guidance on disqualification orders as part of the next round of miscellaneous updates and subject to public consultation. Can you provide a more concrete timeline for this?

The miscellaneous amendments project has an annual timetable to ensure that each year there is an opportunity for the Council to seek views on a series of proposed changes to existing guidelines. The next round of miscellaneous amendments begins in May 2026. As soon as work begins on that project the Council will be invited to consider the inclusion of guidance on disqualification orders.

The likely timetable for the miscellaneous amendments project is a 12-week consultation commencing in early September 2026. Any changes to sentencing guidelines resulting from that consultation would require approval by the Lord Chancellor and Lady Chief Justice so we cannot be sure of the timetable – but we would aim for them to come into force in April 2027.

The consultation aims to seek views on the proposed amendments and may have the effect of raising awareness of the issues amongst consultees.

The Sentencing Council is always pleased to provide information about sentencing and about how the guidelines work. I hope these responses are helpful.

Appendix 7: Response from the Electoral Commission

1 Summary

Recent years have seen a worrying rise in the abuse and intimidation of candidates. This has a significant impact on the individuals themselves and can deter those considering standing, limiting the diversity of candidates and choices for voters.

We welcome the Speaker's Conference on this issue, and the timely and considered recommendations it has made. We are grateful for the opportunity to give and listen to evidence, alongside others, to help build a deeper understanding of the issue and potential solutions.

The UK Government has endorsed the recommendations in the first Speaker's Conference report, and included several of the proposals in its recent strategy paper for modern and secure elections. This is a welcome step, and we are working closely with officials to ensure these changes are workable, and where necessary are made into law.

Since the general election we have worked with partners to offer practical solutions to address this issue. Ahead of the May 2026 elections, we will work with parties to agree principles for a campaigning code of conduct. We will continue to support the police, and will introduce a candidate contact form in nomination packs to support them to share information with candidates in emergencies. We will provide updated guidance to Returning Officers (ROs) on managing disruption at polling stations and counts. We are also piloting new democratic education resources and testing new tools to detect and tackle deepfakes and disinformation. We will survey candidates after the poll, and consult with parties, to continuously test what worked, and inform future responses.

We know that more needs to be done to better understand and address public attitudes to politicians, improve enforcement and understanding of offences, and compel platforms to take action to make their sites safer for campaigners and free from abuse.

This response outlines our position on the recommendations made by the Conference. Where a recommendation is directed to another organisation, and we don't have a position, we have not responded.

2 First report

Code of conduct for campaigning

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. (Paragraph 28)

Electoral Commission response:

- A code of conduct for campaigning will facilitate a robust but respectful campaigning environment by making it clearer that campaigners are accountable for their conduct and by building a shared understanding of what constitutes fair and open campaigning.
- The UK Government has endorsed the Conference's call for a code, including it in its [strategy for modern elections](#). We are keen to work closely with parties and campaigners, the Ministry for Housing, Communities and Local Government, and Mr Speaker to update and expand the existing code of conduct to set the expectations on fair and open campaigning. We recommend that the existing, non-statutory code be strengthened, rather than introducing an additional code, in order to avoid confusion and unnecessary complexity for campaigners.
- This is a significant piece of work, and we have therefore considered what might be possible ahead of May's elections to support our shared objective of a safe and secure campaigning environment for everyone. We will begin by developing a foundational set of respectful campaigning principles.
- We intend to work with parties, through the Parliamentary Parties Panels, to agree a high-level set of principles. We hope to have these agreed in time to guide campaigning at the May 2026 elections. Drafting and agreeing these principles before campaigning begins is dependent on several factors, including parties working collaboratively together. To inform this work, we have requested a copy of parties' own codes of conduct. We will analyse these and identify common themes, which we will consider alongside evidence from this report. To embed and publicise principles ahead of May, we will ask parties, campaigners, and ROs to include them as part of their candidate and agents' briefings. This will help ensure they reach

independent candidates. We will also share principles with local police election Single Points of Contact (SPOC) and Force Elected-Official Advisors (FEOA).

- After May, we will evaluate how the principles worked in practice to develop the detail of the expanded code. A total of 4,515 candidates stood for election across almost 100 political parties at the last general election. For this reason, extensive consultation with a wide range of parties and campaigners will be essential to ensure the code captures and addresses the specific challenges and practical realities of today's rich and varied campaigning landscape.

Disqualification orders

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. (Paragraph 37)

Electoral Commission response:

- We have responded to this recommendation in full in our responses to recommendations in the second report below.

Every police force should produce a fully risk-assessed policing plan ahead of a general election period. (Paragraph 45)

Electoral Commission response:

- Candidate security policing plans would help to address inconsistencies in police responses, by clearly identifying risks and responses ahead of election periods. Election fraud Single Points of Contact (SPOCs) already produce policing plans, using guidance from the College for Policing and the Commission. These plans provide an example of best practice, that could be replicated and used when drawing up security policing plans for general elections. Force Elected-Official Advisors (FEOA) and Bridger SPOCs should work with election fraud SPOCs to share information and ensure co-ordinated responses, since there is often overlap between their work – with some cases including both fraud and security offences.

- Our [research following the UK general election in 2024](#) showed that candidates had mixed experiences with police responses. Candidates told us in our survey following the 2024 general election they experienced inconsistencies in how police forces responded to reported incidents. Some candidates told us that the designated SPOC officers did not contact them, even in hotly contested constituencies where threats had been reported. When they reported incidents, some candidates found police lacked the expertise to handle their complaint, with some allegedly dismissing harassment claims inappropriately as ‘freedom of expression’.
- While robust debate is fundamental, abuse should never be seen as a normal part of the democratic process. We will work with police and Government to ensure that all involved treat allegations and cases of election-related intimidation seriously and demonstrate that those committing offences against candidates and campaigners will face significant sanctions.

Policing

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. (Paragraph 48)

Electoral Commission response:

- We agree. Ahead of the 2026 elections, we are requesting candidates’ contact details as part of nomination packs, and will pass these on to police. This will allow police forces to share essential information with candidates in an emergency. We have provided guidance to Returning Officers (ROs) to make clear they are allowed to share contact details with the police and should do so as soon as possible after the close of nominations.
- Investigating cases of abuse should remain led by the police, since they hold enforcement and prosecution powers that ROs do not. We recognise that, given the complexity of the electoral landscape and

the range of players involved, we have a role to play to support ROs and candidates, by providing guidance, and signposting relevant support.

- Candidates receive security advice from their Force Elected-Official Advisor (FEOA) and specific information on local election management from their local RO. A centralised list of candidates with contact details, such as an email address, would make it easier for police to contact candidates directly. Legislative change may be needed for it to become mandatory for candidates to provide an email address at registration to be shared with the police, as this is currently optional.

Guidance to electoral officials

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. (Paragraph 56)

Electoral Commission response:

- We welcome this recommendation. We produce core [guidance to Returning Officers \(ROs\) on the safe and effective management of all parts of the electoral process](#). We recently updated the guidance on how best to manage attendees at elections, drawing together all the necessary information related to the safety and security of candidates. This includes strengthened guidance on ROs' powers to remove individuals from events when appropriate and around managing behaviours, such as around the use of mobile phones in polling stations and counts, including the filming of proceedings. This will support ROs to manage disruption at electoral events, such as counts, and better protect voters and campaigners from potential abuse.
- We engage closely and regularly with ROs to ensure they are aware of the latest good practice and guidance. This ongoing engagement, guidance and tailored support, underpinned by the agreed principles of our performance standards for ROs, already fulfil the aims of the recommendation here.
- The UK Government has also said it will develop clearer guidance on the application of election, online safety and public order legislation, to be shared with the police, Returning Officers and candidates. Police and RO responsibilities with respect to ensuring polling station security should be made clear, to avoid potential confusion. Polling station security and maintaining public order should remain police-led since they hold enforcement powers, with ROs supported to have clarity about the extent and limits of their responsibilities and jurisdiction.

Clearer guidance from Government will help establish the roles and responsibilities of each of the players involved, ensuring more co-ordinated responses from police, administrators and candidates themselves.

Electoral law review

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.*** (Paragraph 69)

Electoral Commission response:

- Following the Speaker's Conference report, the UK Government has commissioned a review of electoral law in its [election strategy](#) to identify whether there are vulnerabilities and legislative gaps in the powers the police have, considering whether electoral law is sufficient to protect our national security, and finding ways to support the consistency of police responses to these issues across the UK. The Defending Democracy Taskforce will carry out this review, alongside the Commission, and other government departments.
- A review of electoral law will provide an up-to-date assessment of the existing risks and help future proof our democracy against threats. We recommend that it forms part of a wider project to consolidate, modernise and simplify our overly complicated and outdated electoral law, in order to address wider threats facing the electoral system.
- Many of the offences relating to intimidation and harassment are contained within the Representation of the People Act 1983, which does not define key terms, and is based on campaigning practices from 40 years ago. A comprehensive review of the law to identify and address gaps like these would help address this issue and make the law easier to understand and follow.

3 Second report

Public attitudes

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.

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. (Paragraph 30)

Electoral Commission response:

- We strongly share the view that education must play a part in tackling abuse, and that citizenship education should be reformed in order to adequately prepare young people to participate in our democracy.
- Evidence shows us that the earlier a young person starts democratic education, the more positive the civic and political participation outcomes they experience. We recommended democratic education start at primary level in [our submission to the Curriculum and Assessment Review](#). In the lead up to the curriculum's publication in 2027, we will work with the Department for Education, schools and partner organisations to enhance citizenship education. We have also contributed to the curriculum review consultation in Northern Ireland and are working closely with Education Scotland to ensure its reform plans respond to the needs of young voters. We are monitoring the impact of the changes to the curriculum in Wales to ensure it delivers the knowledge, skills and understanding of democracy that young people need in order to participate fully.
- Ahead of elections in May, we will pilot new education resources and projects in formal and informal education settings - from primary to post-16 - to understand which approaches are delivering positive outcomes for young people. We will use this to develop

a democratic education framework that supports schools to prepare students to cast their vote, using the insights gained to contribute to the wider evidence base for implementing votes at 16.

- Our framework will build young people's knowledge and confidence before they cast their first vote. This will include a focus on developing oracy skills to help young people disagree respectfully and argue robustly, media literacy skills to critically engage with political information online, and an understanding of the role of politicians, providing opportunities to connect positively with them. We are also working with partners to include examples of threats to female MPs as part of the Government's strategy to tackle violence against women and girls through education.
- Our resources for teachers will provide guidance on how to deliver lessons in an engaging and impartial way. Teachers have told us they lack confidence in delivering impartial democratic education lessons, with only 78% describing themselves as at least 'somewhat confident' in leading an impartial lesson on democracy and elections. It is essential that teachers trust the material provided, so we'll continue to work with them, alongside parties and other stakeholders, as we develop our impartiality framework.

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. (Paragraph 33)

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. (Paragraph 34)

- Research suggests that positive political contact between young people and politicians increases satisfaction and improves trust in politics. In the last year, we launched a programme of MP school visits. This is part of our strategy to improve democratic education and increase young people's participation in elections and strengthen their confidence in the political system.

- Through these MP visits, we aim to teach young people about their vote, voter registration and the roles and responsibilities of MPs. Our experience of facilitating visits is that they are engaging and useful for young people, helpful and enjoyable for politicians, and can be done in an appropriate non-partisan way. On average, 58% of the students that participate in a workshop with an MP understand more about politics and democracy and 62% feel more confident to register to vote.
- As part of our strategy to support young people voting, we have continued to run '[Welcome to Your Vote Week](#)', which aims to raise awareness of upcoming elections and support first time voting. In 2025 we supported more than half a million young people and nearly 5,000 educators to learn about democracy and voting.

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. (Paragraph 44)

Electoral Commission response:

- Further research into the identities and motivations of perpetrators of abuse will allow for better, more tailored responses to address the issue of abuse and intimidation.
- We have carried out [research into the prevalence of abuse experienced by candidates](#), and are carrying out further research with the public to develop a clearer understanding of where they consider the threshold lies between acceptable and unacceptable behaviour. This can be used to inform future steps relating to policing, campaign behaviour and public education on respectful debate, and treatment of campaigners and elected representatives. We will also continue to survey candidates after every election, to understand their experiences of abuse, and what actions they think should be taken.

The criminal justice response

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.

(Paragraph 106)

- It is vital that each police force has electoral law expertise in order to properly address electoral offences, including those relating to fraud (which are handled by election fraud Single Points of Contact (SPOCs)), and abuse (which are handled by local Force Elected-Official Advisers (FEOAs) and Bridger SPOCs). This helps to ensure that allegations of abuse and fraud are properly dealt with by officers with appropriate expertise, and candidates receive adequate and consistent support.
- Electoral law is highly complex, so in some cases, it may not be appropriate for one officer to hold responsibility as the candidate point of contact for concerns regarding both fraud and abuse.
- The current system, which includes multiple police operations (Bridger and Ford in the UK, and Sandbed for MSPs) and specialised roles (SPOCs and FEOAs) can be complicated for candidates to navigate. Candidates need clear information and guidance about how to access support for both kinds of offence. Police forces should contact candidates at the start of an election, to make clear the relevant contacts they should use for both kinds of offence – be that one point of contact or more than one.
- To help candidates ahead of May, we will be publishing information online, directing candidates to the support and resources they need if they experience abuse, including signposting to support from the police where appropriate.

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.

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.
(Paragraph 132–33)

Electoral Commission response:

- We also welcome the UK Government's decision to introduce a statutory aggravating factor for offences motivated by hostility towards candidates, campaigners, elected representatives, or electoral staff, following recommendations in the first Speaker's Conference report.
- An aggravating factor will help to address the growing problem of candidate security, by enabling increased sentences to both punish offenders and deter future would-be offenders from engaging in intimidation. It will mean that when prosecuting offenders of abuse, courts will have to take the aggravation into account when determining the appropriate sentence – reflecting the seriousness of the offence, and the wider impact abuse has on democracy as a whole. This also helps address the perception among the police that abuse is something they can't get involved with due to concerns around freedom of speech.
- Including offences against electoral staff would extend the protections to a group who are central to delivering elections and have also faced unacceptable abuse, intimidation and harassment. Such a change would also bring reserved elections into alignment with devolved elections in Scotland, where an aggravating factor has recently come into force for offences motivated by hostility towards electoral staff.

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. (Paragraph 141)

Electoral Commission response:

- The 2024 general election was the first general election in which disqualification orders, introduced in the Elections Act 2022 were in place.
- The UK Government has indicated that it intends to extend the disqualification order to cover offences against electoral staff. Currently, these orders only cover offences against candidates, campaigners and elected officeholders. Extending these will help to protect staff from abuse and make polling stations more secure.
- We agree that the UK Government should review the effectiveness of disqualification orders, to ensure police, prosecutors and the judiciary understand, use, and apply them consistently, however we do not think a review should delay disqualification orders being extended.

Social media

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 USUK 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.

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. (Paragraph 190–191)

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.

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.

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. (Paragraph 204–206)

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. (Paragraph 213)

Electoral Commission response:

- Social media and digital platforms have become key tools for campaigners to engage with voters, but growing evidence shows that candidates and voters increasingly face abuse and intimidation when using these platforms. We welcome this Conference's calls to the Government to compel platforms to address harmful content on their sites. Platforms should do more to put in place standardised, rapid-response protocols to remove abusive content and identify perpetrators.
- The Online Safety Act currently requires large platforms to protect content of democratic importance when applying content moderation. We recommend the Government considers creating a clearer new overarching duty on platforms operating in the UK to cover a wider range of risks to elections, to ensure they take action to mitigate risks and protect legitimate political debate, particularly during critical election periods. This would help provide clarity and a shared understanding of what actions are needed by platforms during elections and provide a clearer basis for Ofcom to take enforcement action if appropriate actions are not taken.
- There must not be a higher tolerance for illegal content directed against politicians and public figures compared with others. Our upcoming research (highlighted above) will help provide further evidence about voters' views on the threshold between acceptable and unacceptable behaviour, which could be used to benchmark the effectiveness of moderation policies.
- The Scottish Parliament has developed a pilot scheme to protect elected representatives from online abuse by using targeted keywords and location data to identify potentially abusive content. The pilot has shown promising results, and we are considering with partners how this might be scaled up across the UK. We are also launching a pilot ahead of the May elections to test a deepfake detection tool, focusing on misleading content about the electoral process. The pilot will assess whether suspected videos are deepfakes, analyse their impact on public sentiment, track trends, and inform appropriate regulatory or enforcement action with partners such as Ofcom or the police.
- We continue to meet regularly with Ofcom, including co-ordinating a forum with it and other regulators, working together and responding to shared challenges around elections.

Appendix 8: Letter from Kate Davies, Group Director for Strategy and Research, Ofcom

Thank you for the opportunity to respond to the Speaker's Conference report on the security of MPs, candidates, and elections. The report is a valuable contribution to the debate on how best to keep public figures safe online, particularly during periods of heightened sensitivity such as elections.

In terms of how Ofcom's role relates to the areas explored by the Conference, as the UK's statutory broadcast regulator, Ofcom sets standards for television and radio content through the Broadcasting Code. This includes provisions designed to protect individuals from unwarranted infringements of privacy, including in the way material is obtained, while also respecting freedom of expression and journalism in the public interest. As part of this, our Code sets out several best practices for broadcasters to follow when engaging with individuals, including around the use of doorstepping. Under the Online Safety Act (OSA), Ofcom is also responsible for making sure social media and search firms have effective systems in place to protect adults from illegal content and conduct and additionally protect children from content and conduct that is harmful to them.

The UK's online safety regulation is among the most comprehensive anywhere in the world and the OSA empowers Ofcom with a wide range of investigation and enforcement powers, which we are using to drive change across the sector. We estimate that around 100,000 sites and apps are in scope of the Act, across social media, search, dating, gaming and pornography. The new duties tackle deep rooted failings in sectors that have not considered user safety as they have developed their products. We are seeking a fundamental shift in the tech industry in how firms develop their products and run their services. Our approach is grounded in evidence, gives providers clarity about the actions they need to take, and will adapt as we learn what safety measures prove most effective in a novel field of regulation. The foundations have been laid, but we are under no illusion about the scale of the task that lies ahead. At the beginning of December,

we published our [Online Safety in 2025](#) report which provides practical insights into how we are meeting the challenge of creating a safer life online.

Ofcom recognises that the safety of MPs and public figures is central to a thriving democracy, and this includes the right to an active online presence without their safety being compromised. With a number of elections in the UK in 2026, Ofcom is committed to ensuring companies have effective systems in place to protect users from harm, including to support the safety of public figures. During 2025, we carried out and published research looking into [experiences of online hate and abuse among women in politics](#). We also proposed updates to our Online Safety codes of practice in our [consultation on Additional Safety Measures](#) aimed at reducing the spread of illegal content by making improvements to recommender systems. We also proposed the expanded use of proactive technologies, such as hash matching to block known illegal images, and automated tools to detect harms like fraud, and illegal suicide content.

The attached annex addresses the specific recommendations that relate to Ofcom.

Kate Davies

Group Director for Strategy and Research

Ofcom response to recommendations

*Recommendation 26, Paragraph 71: 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 27, Paragraph 75: 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.*

As set out in [our letter on 01 August 2025](#), Ofcom has several relevant best practices around the obtaining of information and the use of doorstepping. Section Eight (Privacy) of the Broadcasting Code is the most relevant section here and aims to ensure that broadcasters avoid any unwarranted infringements of privacy in programmes and in connection with obtaining material included in programmes. Rule 8.1 reflects the standard set by Parliament that any infringement of privacy in programmes, or in connection with obtaining material included in programmes, must be warranted.³

In addition, Section Eight contains “practices to be followed” by broadcasters when dealing with individuals or organisations participating or otherwise directly affected by programmes, or in the making of programmes. Examples of these practices include a requirement that information which discloses the location of a person’s home or family should not be revealed without permission, unless it is warranted; that when people are caught up in news events they still have a right to privacy in both the making and broadcast of programmes, unless it is warranted to infringe it; that any material likely to infringe a person’s privacy should normally be obtained or broadcast with their consent; and that filming or recording should stop if a person asks, unless there is a clear justification to continue. The means of obtaining material for inclusion in a programme must be proportionate in all the circumstances, and in particular to the subject matter of the programme. These requirements apply to anyone who may be the subject of a story. Failure to follow these practices will constitute a breach where it results in an unwarranted infringement of privacy.

On doorstepping specifically, Section Eight provides that doorstepping for factual programmes should not take place unless a request for an interview has been refused or it has not been possible to request an interview, or there is good reason to believe that an investigation will be frustrated if the subject is approached openly, and it is warranted to doorstep.

“Warranted” has a particular meaning in Section Eight. It means that where broadcasters wish to justify an infringement of privacy as warranted, they should be able to demonstrate why in the particular circumstances of the case, it is warranted. If the reason is that it is in the public interest, then the broadcaster should be able to demonstrate that the public interest outweighs the right to privacy. Examples 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. In applying the Code, Ofcom also takes into account Article 8 (privacy) and Article 10 (freedom of expression) of the European Convention on Human Rights.

3 Section 3(2)(f) Communications Act 2003; Section 107 Broadcasting Act 1996

We acknowledge that the Conference's recommendation calls for these practices to be amended so that doorstepping at residential addresses is treated as a form of harassment with no public interest exemption, and that approaches to children, spouses or other family members should not be used as a means of gaining access to, or information about, MPs or other public figures, again without any public interest exemption.

We consider our practices to be robust and sufficient in protecting individuals from unwarranted infringements of privacy, while at the same time allowing for journalistic freedom in the public interest. Currently we do not have plans to review this particular section of the Broadcasting Code. However, Ofcom periodically undertakes a review of the Code and related guidance to ensure that our rules and regulatory procedures remain effective and relevant. If we consider that changes are necessary, we will conduct an open consultation process. Should a review of the Code be initiated in future, we would welcome the Conference's input through the consultation process.

Recommendation 43, Paragraph 190, Report 2: 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.

It is important that public figures such as MPs and those choosing to stand during election can maintain an active online presence, should they wish to, without being forced to endure hate and abuse.

The OSA is clear that when a service provider is made aware of the presence of illegal content on its service, it is required to take it down swiftly. Our codes of practice set out our expectations about how services should fulfil this duty. The duty applies regardless of who the illegal content is directed at, meaning that services must take down abusive content that is targeted at public figures when they become aware of it.

Since the Illegal Harms duties came into force, we have been scrutinising the steps that services are taking to comply with them, including the take down duty. As set out in our recent report [Online Safety in 2025](#), we will build on this work by determining whether the biggest social media

providers have adequate means of assessing and swiftly removing illegal material that has been reported to them. By April we will have reviewed one major platform's systems, processes and policies for assessing and swiftly removing illegal terror and hate content, including antisemitic and anti-Muslim material. As part of this process, we will use data and intelligence from our research programme, together with information held by civil society and law enforcement partners, and data gathered from platforms. Should this work highlight significant compliance concerns, we will be ready to take enforcement action. We will then extend this work to other services.

Our guidance on [women and girls' online safety](#) makes further best practice recommendations designed to reduce barriers to women reporting online harm (action 8), and to drive services to respond appropriately (action 9). We have written to sites and apps setting an expectation that they start to take immediate action in line with the guidance. We want to see services act on this guidance, which would improve the experiences of female public figures by helping to address the impact of content that is legal but nevertheless hateful or abusive.

Recommendation 44 Paragraph 191, Report 2: 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.

We agree that recommender systems can amplify the impact of harmful content by exposing it to more users, with implications for the targets of the content and others who encounter it.

The OSA requires online services to protect their users from two types of content: illegal content and content that is legal but harmful to children. We already have measures which aim to mitigate the risks of recommender systems in relation to children. Under our Protection of Children Codes, which came into force in July 2025, services have to take steps to protect children from Priority Content, including by reconfiguring their content recommender systems so that this content is not promoted to children. Priority Content refers to the most serious illegal offences such as terrorism, child sexual abuse, hate crimes, and violence. Violent content and content which is abusive or incites hatred are both forms of Priority Content.

Since July we have been driving social media providers to fulfil these requirements. As noted in our Online Safety in 2025 report we will issue formal information requests in early 2026 to find out more. Our information requests are legally binding and failure to comply could lead to enforcement action.

As well as amplifying the impact of content that is legal but harmful to children, recommender systems may also lead to the greater spread of illegal content, including illegal hate and abuse content targeted at public figures. In our [Additional Safety Measures consultation](#) we propose that, where there are indicators that a piece of content might be illegal, service providers should exclude it from recommender systems unless and until their content moderation teams have reviewed it. Where their content moderation teams judge that the content is illegal, it should be removed from the service. Where they judge that it is lawful and allowed on the service they can reinstate it in their recommender systems. We will set out our final decisions on these proposals in our Additional Safety Measures Statement, which will be published in autumn 2026.

We know from [our qualitative research](#) that women in politics face online hate and abuse consistently. The participants in this research told us that the hate and abuse is getting worse, becoming more common, sophisticated and seemingly normalised. The impact of these experiences left the participants feeling isolated, questioning their own abilities and adopting specific tactics to stay safe. We have recently published our final Guidance on a safer life online for women and girls, which gives a series of practical steps that services can take to tackle online gendered harms. Action 6 of the guidance advises services to limit the circulation of content that depicts, promotes, or encourages such harms. For example, platforms should reduce the prominence of misogynistic abuse and sexual violence in content recommendation feeds to minimise widespread dissemination and lower the risk of users encountering this material organically and in large volumes. In 18 months' time we will publish our assessment of the state of women and girls' safety online. The assessment will reveal how effectively services are protecting women and girls and identify gaps that can inform future enforcement and guidance, ensuring our work in protecting women and girls remains responsive and proportionate.

Regarding access to data, in July 2025, Ofcom published the [Researchers' access to information from regulated online services](#), which explored current challenges in how researchers access to data and ways researchers could gain better access to support work on online safety. The report set out three policy options for Government to consider as part of any future access framework. We will continue to work closely with Government on future access initiatives.

Recommendation 45, Paragraph 200, Report 2: 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.*

While we are independent of Government, we are accountable to Parliament. Copies of our Annual Report and Accounts are laid before the UK, Scottish and Welsh Parliaments and the Northern Ireland Assembly. We are subject to review by the National Audit Office and accountable to the Public Accounts Committee for propriety and value for money. We regularly meet stakeholders to discuss our work and to provide clarity about how we approach our regulatory duties.

We regularly give evidence about the full range of work our work to Parliamentary Select Committees across both Houses. In 2025, we discussed our progress in implementing the OSA in six public select committee evidence sessions in Parliament. We have also met with multiple APPGs and individual parliamentarians and convened our own parliamentary events to provide opportunities to discuss and explain our work. In addition to presenting and discussing our work at parliamentary events and evidence sessions, we provide written updates to Parliament whenever we release a major consultation or policy statement, in order to maximise the opportunity for parliamentary engagement and scrutiny. This correspondence can be found on our [website](#). We receive a significant number of letters from MPs raising their constituents' concerns about online safety. Responding promptly and providing the latest updates on our work is a key priority for Ofcom. In 2025, we replied to 57 MP letters, many of which resulted in further constructive discussions.

We also regularly update our Online Safety implementation Roadmap to ensure Parliament and the public have the most up-to-date overview of how we are implementing the OSA. Since October 2023, we have published five updates to our Roadmap, most recently in November. We send these updates to select committees and publish them on our [website](#).

The OSA also gives Ofcom a series of statutory reporting obligations. For example, next year we must publish reports into the use of age assurance and content harmful to children. In 2026 we will provide an annual review of what we have done in response to the Statement of Strategic Priorities in Ofcom's Annual Report and Accounts. In addition to our formal reporting requirements, we have committed to reporting on how industry is responding to its duties and Ofcom's priorities for the year ahead, including our first such [report](#) published on 4 December 2025. We intend this to be a valuable, additional resource for parliamentarians seeking to understand and scrutinise Ofcom's implementation of the OSA.