**INTIMIDATION IN PUBLIC LIFE REVIEW FOLLOW UP**

**RECOMMENDATION TRACKER FURTHER INFORMATION**

Up to date as of 17 December 2020

|  |  |  |
| --- | --- | --- |
| **Recommendation** | **Responsibility** | **More information** |
| Government should bring forward legislation to shift the liability of illegal content online towards social media companies. | Government | [The Online Harms White Paper establishes a new regulatory framework for online safety and sets out a range of legislative and non-legislative measures for tackling online harms](https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#part-2-regulatory-model), including a statutory duty of care to make companies take more responsibility for the safety of their users and to tackle harm caused by illegal and harmful content on their platforms. [This will be overseen by an independent online harms regulator, which will set clear safety standards, backed up by reporting requirements and enforcement powers](https://www.gov.uk/government/news/government-minded-to-appoint-ofcom-as-online-harms-regulator). |
| The government should consult on the introduction of a new offence in electoral law of intimidating Parliamentary candidates and party campaigners. | Government | [In May 2019, the government announced a range of new measures intended to safeguard UK elections from intimidation, influence and disinformation](https://www.gov.uk/government/news/government-safeguards-uk-elections). As well as committing to legislate to introduce a new electoral offence of intimidating candidates or campaigners, the government has committed to:   * legislate to clarify the electoral offence of undue influence of a voter; * implement a digital imprints regime for online campaigning material; and * launch a consultation on electoral integrity. |
| The government should bring forward legislation to remove the requirement for candidates standing as local councillors to have their home addresses published on the ballot paper. Returning Officers should not disclose the home addresses of those attending an election court. | Government | The government made four statutory instruments that removed the preexisting requirement for candidates at local, parish and mayoral elections to publish their home addresses during the election process and be included on the ballot paper at these polls. A candidate may now choose that their home address is not made public and that the local authority area in which they live appears on the ballot paper instead. |
| Political parties should set clear expectations about the behaviour expected of their members, both offline and online through a code of conduct for members which specifically prohibits any intimidatory behaviour. Parties should ensure that members are familiar with the code. The consequences of any breach of the code should be clear and unambiguous. | Political parties | [In 2019, the Committee reviewed the codes of conduct of political parties holding seats in Westminster, considering scope, themes and language.](https://www.gov.uk/government/publications/intimidation-in-public-life-review-of-political-parties-codes-of-conduct) The party codes all prohibit bullying, harassment and unlawful discrimination – conduct that clearly falls within the scope of intimidation. Some of the codes list further categories of behaviour that will not be tolerated by parties, including victimisation, abuse and hateful language. As well as precluding poor behaviour, many of the codes refer explicitly to the positive behaviours expected by party members – fairness, respect, tolerance and dignity are common themes. Several of the codes also include the expectation that members will challenge unacceptable behaviour where it occurs. The codes vary in their approach to referring to procedures for alleged breaches of the code. |
| Political parties must ensure that party members who breach the party’s code of conduct by engaging intimidation are consistently and appropriately disciplined in a timely manner. | Political parties | A range of sanctions are included in parties’ disciplinary frameworks, should any member breach their party’s code of conduct. These include: formal warning; reprimand; suspension from party membership; prohibition from holding office or standing for election to any specified party role, permanently or for a specified period; and revocation of party membership. It is not clear to what extent parties enforce the full range of sanctions available to them to discipline intimidatory behaviour by their members. |
| Political parties must collect data on the number of complaints against members for engaging in intimidatory behaviour, and the outcome of any disciplinary processes which result from these complaints. | Political parties | See correspondence from [the Liberal Democrats](https://www.gov.uk/government/publications/intimidation-in-public-life-letters-from-the-liberal-democrats); [the Labour Party](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757910/Labour_Party_Response_Intimidation_in_Public_Life.pdf); and [the Green Party](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-green-party). The Committee has not heard from other parties on this issue. |
| The political parties must work together to develop a joint code of conduct on intimidatory behaviour during election campaigns by December 2018. The code should be jointly enforced by the political parties. | Political parties | The Committee has been working with The Jo Cox Foundation since 2019. We have been working with political parties to draw up a common statement of principle on intimidatory behaviour to encourage cross-party consensus on the issue. Our work to date has evolved through close collaboration with the political parties and draws on the language of existing party codes. The resulting statement is not intended to supersede or replace party codes of conduct or disciplinary processes, but to complement them by acting as a high level statement of principle outlining the minimum standards of behaviour that all party members should aspire to.  [See the joint statement on conduct of political party members here.](https://www.gov.uk/government/publications/intimidation-in-public-life-joint-statement-on-conduct-of-political-party-members) |
| Political parties must take steps to provide support for all candidates, including through networks, training, and support and resources. In particular, the parties should develop these support mechanisms for female, BAME, and LGBT candidates who are more likely to be targeted as subjects of intimation.  Political parties must offer more support and training to candidates on their use of social media. This training should include: managing social media profiles, block and mute features, reporting content, and recognising when behaviour should be reported directly to the police. | Political parties | See correspondence from [the Liberal Democrats](https://www.gov.uk/government/publications/intimidation-in-public-life-letters-from-the-liberal-democrats); [the Labour Party](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757910/Labour_Party_Response_Intimidation_in_Public_Life.pdf); [the Conservative Party](https://www.gov.uk/government/publications/intimidation-in-public-life-letters-from-the-conservative-party); [the Green Party](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-green-party); and [Plaid Cymru](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/700862/Letter_from_Plaid_Cymru.pdf). The Committee has not heard from other parties on this issue. |
| The National Police Chiefs Council should ensure that local police forces have sufficient training to enable them to effectively investigate offences committed through social media. Local police forces should be able to access advice and guidance on the context in which MPs and Parliamentary candidates work. | National Police Chiefs Council | [The **NPCC** has established a network under Operation Bridger, the mechanism by which the Parliamentary Liaison and Investigation Team supports single points of contact within each police force area.](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-npcc)The Parliamentary Liaison and Investigation Team use this network to disseminate knowledge and learning to single points of contact across the country. This includes advice and guidance on the current threat picture for MPs, the context of the political landscape and other emerging issues, including online activity against MPs. |
| The College of Policing Authorised Professional Practice for elections should be updated to include offences relating to intimidation, including offences committed through social media. | College of Policing | [The Authorised Professional Practice for elections sets out the key roles for the police service and other agencies who need to work together to ensure an effective police response to elections, including their responsibilities for recognising and responding to harassment, intimidation or threatening behaviour.](https://www.app.college.police.uk/app-content/policing-elections/key-roles-and-planning/) |
| The National Police Chiefs Council, working with the Crown Prosecution Service and the College of Policing, should produce accessible guidance for Parliamentary candidates giving clear advice on behaviour they may experience during a campaign which is likely to constitute a criminal offence. | National Police Chiefs Council, working with the Crown Prosecution Service and the College of Policing | [The guidance was updated ahead of the 2019 General Election. It includes key indicators, offences and ways to protect yourself, legal definitions and what might constitute a breach of criminal law.](https://www.electoralcommission.org.uk/sites/default/files/2019-11/Joint%20Guidance%20for%20Candidates%20in%20Elections%202019.pdf) A copy of the guidance was disseminated to political parties and returning officers during the General Election and briefings were held in each police force area for candidates. |
| Social media companies must develop and implement automated techniques to identify intimidatory content posted on their platforms. They should use this technology to ensure intimidatory content is taken down as soon as possible. | Social media companies | **Twitter, Facebook** and **Google** are increasingly using technology like machine learning to scale the efforts of human moderators and proactively identify, review and remove content that violates their policies:   * [During the reporting period January to June 2019, more than 50% of Tweets that **Twitter** took action on for abuse were proactively identified using technology](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/858847/Intimidation_in_Public_Life__Letter_from_Twitter_6_December_2019.pdf); * [The proportion of hate speech removed by Facebook before it’s been reported has tripled since 2017](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/858825/Intimidation_in_Public_Life__letter_from_Facebook_12_December_2019.pdf); and * [Between April and June 2020, **Youtube** removed 11.4 million videos for violating their guidelines. 10.8 million of those were flagged by machines, with 42% not receiving a single view](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-google). |
| Social media companies must do more to prevent users being inundated with hostile messages on their platforms, and to support users who become victims of this behaviour. | Social media companies | All three social media companies have measures in place to protect their users from intimidation and harassment. These include policies and guidelines that outline what is and is not allowed on their platforms; mechanisms to detect and remove abusive content; and reporting channels for users to report content and behaviour that violates their policies.  See correspondence from [Twitter](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-twitter), [Facebook](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-facebook) and [Google](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-google). |
| Social media companies must implement tools to enhance the ability of users to tackle online intimidation through user options. | Social media companies | **Twitter, Facebook** and **Google** give users a range of options to control the content they see, what others see and who they can interact with online. These include advanced filter settings that allow users to disable notifications from certain types of accounts, and block, mute and safe search functions. For example:   * [In August 2020, Twitter made conversation controls available to all users. This means that before you Tweet, you can choose who can reply](https://blog.twitter.com/en_us/topics/product/2020/new-conversation-settings-coming-to-a-tweet-near-you.html) (everyone; only people you follow; or only people you mention); * [People who manage Facebook pages, like those for candidates, can hide or delete individual comments. They can also moderate posts by turning on the profanity filter or by blocking specific words that they do not want to appear on their page](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757908/CSPL_-_Facebook_Additional_Written_Evidence.pdf); and * [Account holders on Youtube can delete, turn off or manage comments on their videos by requiring pre-approval before they are posted publicly.](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-google) |
| All social media companies must ensure they are able to make decisions quickly and consistently on the takedown of intimidatory content online. | Social media companies | All three social media companies have measures in place to ensure they’re able to make decisions quickly and consistently on the takedown of intimidatory content. This includes using both human moderators and machine learning systems to identify and remove harmful content at speed, often before users have seen it; increasing the number of people working to address content that might violate their policies; and providing tools for users and organisations to report intimidatory content.  See correspondence from [Twitter](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-twitter), [Facebook](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-facebook) and [Google](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-google). |
| Twitter, Facebook and Google must publish UK-level performance data on the number of reports they receive, the percentage of reported content that is taken down, and the time it takes to take down that content, on at least a quarterly basis. | Social media companies | **Facebook** and **Google** both publish quarterly transparency reports on the number of reports they receive and the amount of content they take down. **Twitter** publishes transparency data biannually, as below:   * [Facebook’s transparency reports include a Community Standards Enforcement report that publishes data on the amount of content taken down and a proactive removal score that shows how much content was found before it was reported.](https://transparency.facebook.com/community-standards-enforcement) It now includes a report on the amount of content actioned for violating their bullying and harassment policy; * [Youtube’s transparency report provides aggregate data about the flags they receive and the actions they take to remove videos and comments that violate their policies.](https://transparencyreport.google.com/youtube-policy/removals?hl=en_GB) It also breaks the data down by country or region. [Google also publishes a broader transparency report for their services, detailing the number of requests they have received from government or law enforcement to remove or delist content](https://transparencyreport.google.com/?hl=en_GB); and * [Twitter has recently launched a transparency centre, which covers an array of transparency efforts, including information requests, removal requests, copyright and trademark notices, email security and platform manipulation](https://transparency.twitter.com/). [It also includes a rules enforcement report, which publishes data about the number of accounts actioned and suspended and the amount of content removed for breaching their rules](https://transparency.twitter.com/en/reports/rules-enforcement.html#2019-jul-dec). |
| Social media companies must urgently revise their tools for users to escalate any reports of potential illegal online activity to the police. | Social media companies | **Twitter** and **Facebook** both have guidelines for law enforcement to support their work but do not provide adequate advice to users on how to escalate illegal online activity to the police. [Their guidance on reporting abusive behaviour and content tends to advise users to “contact [their] local law enforcement agency”, which does not help them to constructively engage with the police when they’re facing illegal abuse online.](https://help.twitter.com/en/safety-and-security/report-abusive-behavior)  [**Google** said that **Youtube** operates a “notice-and-action system” for users and government authorities to report content which may be unlawful in local jurisdictions. They provide a tool to help users report content they believe should be removed from Youtube based on applicable laws](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-google). |
| The social media companies should work with the government to establish a ‘pop up’ social media reporting team for election campaigns. | Social media companies | **Twitter, Facebook** and **Google** all established temporary election teams during the 2019 General Election to protect the integrity of election-related content and identify and respond more quickly to potential threats and challenges, including removing intimidatory content. [Facebook has since established a permanent reporting channel for MPs to flag any abusive or threatening content, which runs year round for sitting MPs and is extended for Parliamentary candidates during elections](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/858825/Intimidation_in_Public_Life__letter_from_Facebook_12_December_2019.pdf). All three companies also have “trusted flagger programmes”, which allow organisations like the UK Parliament’s *Members’ Security Support Service* to expedite reports directly to them. |
| Social media companies should actively provide advice, guidance and support to Parliamentary candidates on steps they can take to remain safe and secure while using their sites. | Social media companies | **Twitter, Facebook** and **Google** all work closely with the Parliamentary authorities, political parties and the government to ensure that MPs and candidates are properly supported when it comes to staying safe online.  [Ahead of the UK General Election in 2019, they published joint candidate safety guidance on the types of content and activities that breach services’ terms and conditions and how candidates can report content that violates their policies.](https://uk.internetassociation.org/blog/resource-for-parliamentary-candidates/) All three companies shared bespoke election and safety resources with sitting MPs, political parties and the government. [Twitter also said they offer safety and security training for parties and candidates and drop-in sessions for MPs and their staff](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/858847/Intimidation_in_Public_Life__Letter_from_Twitter_6_December_2019.pdf). |
| Press regulation bodies should extend their codes of conduct to prohibit unacceptable language that incites intimidation. | Press regulation bodies (IPSO and Impress) | [In 2020, the Committee followed up with the Editors’ Code of Practice Committee on why they would not be amending the Code.](https://www.gov.uk/government/publications/intimidation-in-public-life-letter-from-ipso) They said that:   * The press regulated by IPSO should not be held responsible for the activities of unregulated individuals acting as online trolls and a change to the Code would unduly restrict freedom of expression and the right of the press to report and comment on public affairs; * Editors exercise discretion for their own editorial content and use of language and they are open to criticism and are called to account by their readers and those in public life. The Code does not and should not seek to dictate the language of journalism, which is entirely a matter for editors, who must comply with the Code and the law; * The Editors’ Code seeks to balance both the rights of the individual and the public's right to know. It states that it should be interpreted “neither so narrowly as to compromise its commitment to respect the rights of the individual, nor so broadly that it infringes the fundamental right to freedom of expression – such as to inform, to be partisan, to challenge, shock, be satirical and to entertain – or prevents publication in the public interest.” It is in the interests of everyone that the press is free to campaign, scrutinise and criticise those exercising the power of the state. Those rights are balanced by responsibilities and the Code offers protection to individuals, including those in public life. |
| News organisations should only consider stories from freelance journalists that meet the standards of IPSO’s Editors Code, or the Editorial Guidelines of Impress, as appropriate, and ensure that freelance journalists are aware of this policy. | News organisations | [The preamble to **IPSO’s** Code of Practice says that *“It is the responsibility of editors and publishers to apply the Code to editorial material in both printed and online versions of their publications. They should take care to ensure it is observed rigorously by all editorial staff and external contributors, including non-journalists.”*](https://www.editorscode.org.uk/the_code.php)  [The Editors’ Codebook, which explains how the Code is interpreted and enforced by IPSO, has examples of how this is effective in the section devoted to the preamble.](http://editorscode.org.uk/downloads/codebook/Codebook-2020.pdf) |