Online Security Information for Candidates
General Election 2019

Most social media companies provide advice about online security. This includes how to secure your account and how to report online abuse, intimidation and threats. Social media companies are taking steps to secure their platforms and users against misuse during the 2019 General Election.

Guidance and resources from platforms can be found here on the Internet Association Website here:
https://uk.internetassociation.org/blog/resource-for-parliamentary-candidates/

Please also see specific guidance for candidates and their staff from Twitter, Facebook, Google and YouTube below.

Twitter

Safety is our priority; and more than 50% of Tweets we take action on for abuse are now proactively surfaced using technology. As we seek to further reduce the burden on victims, we also want to continue to partner with key stakeholders and ensure all candidates are provided with key information on our rules, reporting and safety tools. Below is some important information from Twitter regarding the General Election.

- **Username swaps:** We can facilitate the swapping of your username for the election; and the freeze of your current username. This service is designed for MPs who are running for re-election. Please email govuk@twitter.com with your current username and desired username, and we will process as soon as possible.

- **Resources:** Our short guides to campaigning and staying safe on Twitter are available on the Internet Association website.

- **Reporting:** Reporting in-app or via our website is the most efficient way of reporting potential violations of our rules - you can find further information here.

  The Partner Support Portal is an exclusive page in the Twitter Help Center that provides elevated support to partner organisations. We have contacted the main political parties to ensure all key organisations not already onboarded are given the opportunity to join.

  Separately, we can be contacted by candidates via govuk@twitter.com with any questions; we would, however, advise users to report on Twitter directly first and then send through the case number. This will help expedite the process.

- **Webinars:** We will be holding webinars throughout November for candidates and campaigners covering Twitter best practice; security; safety; and Q&A. They will be held on 22nd November (12-1pm), 25th November (10-11am) and 28th November (1-2pm). If you are interested in attending, please email govuk@twitter.com, indicating which session you would like to attend.

Facebook

As a candidate standing in the upcoming general election, we wanted to share with you information on how to have a safe experience on the platform during the campaign, and how to report threatening or harassing content to us. To that end, please find below information on how to report via the platform, and via the dedicated reporting channel which is available to you as a candidate. This channel is for use by candidates and their staff to flag content of particular concern.

We also want to highlight the [Facebook Safety Guide for Page Admins](#), which provides guidance on protecting your own Page and the tools available to do so.

- **Reporting and removing content:** Every piece of content on Facebook and Instagram has a report button, and in addition to removing content that violates our [community standards](#) (what is and isn't allowed on Facebook) we refer cases to law enforcement when we become aware of an imminent threat. Our Community Operations teams are available 24/7, and we now have 35,000 people worldwide working on safety and security. We are also investing more in automated techniques for content removal to help us remove as much of this content as quickly and proactively as possible. To report via the platform, please use the report button, ensuring that you follow the process to the point of submitting a report after you have provided feedback.

- **Contacting Facebook and Instagram:** As well as the report function available on every piece of content on Facebook and Instagram, we want to ensure you can raise any concerns around content to the Facebook Politics and Government Outreach team directly via this email address - ukpol@fb.com. Should you have any concerns relating to abuse or content on the platform and its impact on your role as a candidate, please do not hesitate to get in touch via this channel. Included below is a template email which you can use when reporting content via this email address, to ensure it is able to be investigated as quickly as possible by our teams. This channel is for use by candidates and their staff only at present.

- **Managing your account and Page:** To help ensure that negative content does not appear on your Page in the first place we have developed a range of tools that allow public figures to moderate and filter the content that people put on their Pages. People who help manage Facebook Pages can hide or delete individual

comments. They can also proactively moderate comments and posts by visitors by turning on the profanity filter, or blocking specific words or lists of words that they do not want to appear on their Page. Page admins can also remove or ban people from their Pages using the straightforward tools available to them as administrators. Details of how to apply these measures is included in the Safety Guide for Page Admins. We also have a publicly available website, www.facebook.com/gpa which provides insight and advice on best practice across a range of areas, including protecting account safety and security.

- For issues including account verification, support on ads and general support on non-urgent issues, you have access to our dedicated support team. Please go to www.facebook.com/gpa/help and use the form to contact our support team directly.

Template for reporting via inbox:

Name:
Please give your full name

Title:
Please give your title: (e.g. x candidate for x constituency)

What are you reporting? (delete as appropriate)

- This user is harassing me
- I believe this user is harassing someone else
- I believe this user is a danger to me or someone else
- I believe this user is violating your Community Standards
- I believe this content has potential for real world harm

Please provide a brief description of the issue and why you believe it violates our community standards (outlined here):

Violation Link on Facebook or Instagram:
Please provide full URL links for our team to review (link to the actual page for a page review, link to the exact photo for a photo review). Please only provide links to Facebook content (We cannot act based on links or screenshots of content from other

online providers)

Screenshots for comments/posts/photos:
Specific piece of content you are concerned about if you cannot find the link

If this is about ongoing user harassment, can you tell us when this harassment started?
i.e. one week ago/one month ago

In the case of a long video, please provide exact time of abuse:
For example, graphic violence at 5.35mins

Other context or links to external content:
Provide a reason or full context for the flagged content like a police reference, case number, activity on other platforms or elsewhere on the Internet, media reports

Please let us know if this content has been reported before:
Yes/No

How to provide URLs to us:
- In order for us to accurately investigate your report, we need to understand the specific piece of content you believe to be in violation of our Community Standards. This can only be done if you provide the URL to the specific content at issue.
- URLs of posts, photos, videos or comments can be generated by clicking on the time or date on which content has been posted and then copying the link in the web bar at the top of the page.
- For example, sometimes pages may contain violating content, but it may be a particular post rather than the entire page that contains violating content. Therefore, in order for our team to investigate you can provide us with a URL to the specific post by following these instructions.

Google

Online security takes many forms: information security - protection against threats from those who want to access data maliciously or disrupt the flow of information - and personal security, against those who would use online platforms to target or abuse specific individuals. Whilst we know technology alone can't solve the issue, we invest in creating and maintaining the infrastructure to keep our users' accounts and websites secure, and to protect them from content that violates our guidelines.

If you have a Google account, YouTube channel, or host a website, we would be delighted to offer you and your team in-person training on how the different features and measures we have developed work, for example:

- **How to protect your email against phishing attempts**, by using our Advanced Protection Programme. This system uses a physical security key, to offer the most sophisticated protection yet against those who would try to access your data illegally. We would be happy to offer you your first key to enable you and your office to take advantage of this higher level of security.

- **How to protect your constituency website from DDoS attacks** - digital attacks which can be used to take your website offline - by installing our Project Shield tool, which has been designed to address this kind of malicious attack and can be installed in approximately ten minutes.

- **How to access the enhanced moderation controls** on YouTube, which help you manage comments on your channel. YouTube account holders can delete inappropriate comments and block a user so they can't view videos or leave more comments. Comments can also be turned off for any video by the uploader or managed by requiring pre-approval before they are posted publicly.

- We can also talk in detail about **how to flag content that violates our Community Guidelines** on YouTube, and the action that our teams take to ensure that our platform does not contain abusive content.

We know that the abuse of people in public life is a concern to many in Parliament, and we have been actively working with partners including the Metropolitan Police and the Parliamentary Security Department to identify and respond to this issue. If a briefing on these issues would be of interest, or you would like a physical security key, please do get in touch on ukpublicpolicy@google.com.

YouTube

At YouTube, we have Community Guidelines that set the rules of what is not allowed on the platform. We remove content that violates these guidelines, whether in videos or comments. Hate speech, predatory behaviour, graphic violence, malicious attacks and content that promotes harmful or dangerous behaviour isn't allowed on YouTube. Among others, we have policies that cover:

● **Hate Speech:** We remove content promoting violence or hatred against individuals or groups based on any of the following attributes: age, disability, ethnicity, gender identity and expression, nationality, race, immigration status,religion, sex/gender, sexual orientation, victims of a major violent event and their kin, and veteran status

● **Harassment and Cyberbullying:** Content or behaviour intended to maliciously harass, threaten or bully others is not allowed on YouTube.

● **Harmful or Dangerous Content:** Content that aims to encourage dangerous or illegal activities that risk serious physical harm or death is not allowed on YouTube.

Please report content that violates our policies. Instructions for reporting violations of our Community Guidelines are available here. If you need to report more than one piece of content or wish to submit a more detailed report for review, use the reporting tool. This can be used to highlight a user's comments, videos and provide additional information about any concerns. The in-product reporting tool can be used for targeted abuse.

Once content has been reported, YouTube's Trust & Safety team reviews it. Reviewers evaluate flagged videos against all our YouTube Community Guidelines and policies. If a video is found to violate our policies, it will be removed from YouTube. If a strike is particularly egregious or a whole channel is found in violation of YouTube's Community Guidelines, we may remove the channel and its videos immediately. Comments can be turned off for any video by the uploader or managed by requiring pre-approval before they are posted publicly.

Full details on the comment moderation features can be found here. You can also contact our team directly at ukpublicpolicy@google.com.