Personal Safety for Elected Members

Introduction

Our personal safety is something many of us take for granted, and it is only when a major incident occurs that we stop and think about our own vulnerability. The recent murder of MP Jo Cox will have caused even the most confident amongst us to take a step back to reflect on the way that we manage any risks associated with our role.

There have been very few major incidents involving violence toward local or national politicians, although when attacks do take place they are widely reported. There are no statistics to prove that public figures are at more risk than anybody else who is involved in carrying out a front-facing role.
Whilst most of the aggression councillors experience will usually sit at the 'low to modest' spectrum of unacceptable behaviour, severe abuse can tip into the legal definition of violence even if no physical interaction is involved.

We should all take time out of our busy schedules to reflect on the systems and processes we should have in place to help keep us safe, and to reduce any risks we may be exposed to in our councillor role.
Below is some information that has been compiled from LGIU and LGA guidelines. For more information, visit the government website: **www.hse.gov.uk/risk/casestudies/**

General principles of personal safety

There are four broad principles to consider linked to personal safety:

1. Organic risk assessment
2. Gut feel
3. Early choices
4. Routine

1. Organic risk assessment

Organic risk assessment is more focused on assessing risk in the here and now, based on the signals we are picking up from our environment.
It is generally believed that a person who is new into a role is much better at identifying and assessing risk than somebody else who has been carrying out the same activity for a period of time who can sometimes become complacent.

2. Recognise and use your gut feel

No risk assessment can replace using our own senses to determine what feels safe, versus what feels wrong. This is often referred to as 'gut feel'.
Unfortunately, as adults we often silence our gut feeling in an attempt to intellectualise it. In personal safety terms, gut feel is one of the most important tools we have.

Remove yourself immediately from the situation if you feel unsafe, analyse later but your immediate safety is the priority.

3. Early choices

Early choices are conscious decisions we make about our personal safety that can help to protect us if we have a problem.
De-briefing people who have been involved in events where their personal safety has been compromised, and it is estimate that most, if not all, have expressed regrets about early choices they could have made – and didn't.

4. Routine

Routine is often described as the enemy of personal safety because it makes our behaviour predictable and reliable. Whilst reliability is often a prized characteristic, in safety terms it can make us vulnerable, particularly when an habitual activity is known to others.
Whilst it isn't always possible or practical to vary patterns a huge amount, when you are able to do so, change your routine so that you vary the time and places you do things.

Handling intimidation

Introduction

This document is not designed to alarm, but to suggest some steps you can undertake to protect yourself as a person in a public position, and how to respond should an incident occur.

The most important determining factor in deciding how to respond to intimidation is the impact it is having on you. Regardless of what others may think, if it is having an effect on you, then that is sufficient for you to take action.

Key points:

- Councillors are encouraged to keep a record of any intimidatory communication or behaviour
- Contact with unknown or anonymous individuals should be undertaken with care

General advice

Below are a suggested set of actions that you could undertake if you consider you are being subjected to intimidation:

- Make sure that your immediate safety is not at risk. Make sure you are safe.
- If possible, record or diarise the encounter or communication. In the case of an email or letter, you can copy or save it. A telephone call or face-to-face discussion and social media incident should be written in a diary as soon as possible after the event, recorded, screen-shot or saved. You can also take photos of damage or even a computer screen. Even if this is the first or only incident, others may also have been subjected to intimidation. A collective record is important if future action is

going to be taken. It is also important that incidents relating to the same individual or individuals should be recorded as such evidence could be critical should the matter gives rise to a criminal prosecution.

- Raise the incident with a view to discussing it or obtaining support from a nominated council officer and/or political group nominated person. This will also help you establish if others have been subjected to the same or similar intimidation.
- If a serious potential crime has occurred, it is advisable to formally report it to the council and/or to the police, particularly in the context of a serious threat to life or anticipated violence.
- If you are concerned about your personal safety, raise this with the council and the police so that there is a record of the impact the incident is having and review your own security and personal safety. This could include your personal or work activities and those of your family.
- Under the Health and Safety at Work Act, councils have a duty to safeguard their staff against potentially violent persons and BwDC maintain a Caution list with names of such parties. This will enable you to ascertain if the individual or individuals who have intimidated them are on the Caution List, if not; ensure that that their name is added using the appropriate processes.
- Every situation will be different, and it will need a personal judgement about whether it is worthwhile to pursue the incident, ignore it or politely acknowledge.
- If the letters or emails continue further steps may need to be considered such as advising the individual that such abuse will result in a referral to the police and the stopping of further correspondence.

Shield Principles

In addressing public intimidation, the LGA has developed the following SHIELD principles:

Safeguard – where possible, protect yourself online and in person. For example, set out in any online biography or page that abusive, threatening or intimidatory communication or actions will be reported, utilise security features, take personal safety precautions and have a point of contact in the local police for any incidents.

Help – in any situation ensure you are safe before you take further action and get help if needed. If the threat is not immediate, you can contact officers at the council who have been given the responsibility to support you or someone with that role from your political group.

Inform – you can inform the individual or group that you consider their communication or action as intimidating, threatening or abusive. There is a growing movement of 'digital citizenship', which encourages the labelling of poor online conduct as a way of challenging such behaviour.

Evidence – if you consider that a communication or action is intimidatory, threatening or abusive, gather evidence. For example, photos, recordings, screen-shots, letters, emails, details of witnesses, etc.

Let people know – report the incident to your social media platform/officers/party contact/lead member/the police, depending on the nature and severity of the incident(s). Be prepared that the police

and courts will look to determine if the incident is intimidation based on the theoretical opinion of the average person.

Decide – determine whether you want to continue receiving communications from the individual or group and block or mute if on social media where appropriate. Decide if you want to pursue any action to inhibit the ability of the individual or group to approach you.

Specific safety tips

A number of safety tips have been compiled from a variety of sources including guidance from councillors, which have been shared during training sessions. They relate to the different activities councillors are involved in as part of their role and come from the Police and from personal safety agencies. Most of the approaches are simply common sense. The full list can be found at the end of this document.

You must always check the Caution list located on the Intranet here prior to any visit or meeting with someone not known to you.

Incident reporting

If you are involved in an incident, or have concerns around an individual's behaviour, it is important to report this to the Democratic Services team.
An incident report must be completed as soon as possible after an event, whilst memories are fresh and so that issues can be investigated and appropriate action taken. This should be forwarded to the Health and Wellbeing team.

If the incident involves acts of a potential criminal nature the Police Authority have created a helpful guide to understanding what constitutes criminal acts and how you can report this. You can access this information by clicking the link below:

https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Joint-Guidance-for-Candidates-in-Elections.pdf

- This link provides information about common cyber attacks seen against those in politics, and suggests preventative measures https://www.ncsc.gov.uk/guidance/guidance-for-individuals-in-politics. .
  Key Contact Information: Report an incident - report.ncsc.gov.uk or incidents@ncsc.gov.uk ;
  Enquiries: enquiries@ncsc.gov.uk

Social Medial companies have also provided guidance on online security and how to report incident. This guidance can be accessed using the links below

- Online Security Information for Candidates (Appendix 1)
  Key Contact Information: Twitter: govuk@twitter.com; Facebook: ukpol@fb.com;
  Google and YouTube: ukpublicpolicy@google.com

Other sources of help

One of your key sources of help should be the council's safety procedures. These will include policies around Lone Working, and general support associated with safety in the councillor role.
The Suzy Lamplugh Trust is particularly well known for the quality of their advice. Their website is: http://www.suzylamplugh.org.

We also offer the following me-learning courses:

- Angry customers
- Assert yourself
- Challenging behaviour
- Dealing with Sensitive Issues
- Emotional abuse
- Handling complaints
- Handling difficult situations
- Managing challenging behaviour effectively
- Managing conflict
- Satisfying challenging customers
- Under pressure

These courses can be located on the Blackburn with Darwen Learning site here .
To view these courses go to the course library, select online courses and a list of all online courses will appear. The above courses can be searched for by using the search bar on the right hand side of the page.

And finally

Please remember, we live in a world where by far the majority of people are friendly and gentle, and where many kind acts go unnoticed and unreported.
Personal safety is about taking sensible steps to minimise risk, so that we are confident and comfortable in our councillor role.

Appendix 1
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 Centre that provides elevated support to partner organisations. We have contacted the main political parties to ensure all key organisations not already on boarded 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 towww.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, and 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