



Llywodraeth Cymru
Welsh Government

Protecting your organisation from hate and harassment

A Practical Guide

Contents

Quick reference cards	3
Part 1: Understanding the threat landscape	4
How campaigns against organisations typically develop	4
What counts as harassment vs. free speech	5
When is it misinformation, disinformation or something else?	5
Part 2: Prevention strategies	7
Digital Security Audit tool	7
Social media platform help and settings	8
Event planning security considerations – Questions to ask	9
Staff training basics – Tips about what everyone should know	10
Part 3: Incident response procedures	11
Immediate response actions – What to do if targeted	11
Documentation Templates – How to record incidents effectively	13
Part 4: Communication strategies	14
Social media platform dynamics and user behaviour	14
Moral Foundations Theory	14
Alternative narrative rather than counter narrative	15
Proactive partnerships	15
Part 5: Support directory	16

The Welsh Government acknowledges that the technology, platforms and approaches referred to in this guide continue to develop quickly. We offer our current suggestions about ways to safeguard staff and service users, whilst maintaining freedom of expression in support of community cohesion. This guide does not suggest a ‘correct’ or ‘wrong’ way to confront these problems.

Quick reference cards

“Before It Happens” Checklist

- **Do the basics:** Set up Two-factor authentication (2FA) across all accounts, limit admin access, set strong passwords.
- **Review your digital footprint:** What personally identifiable information exists about staff online? Is it essential or can it be removed?
- **Prepare your team:** Do they know what to do if they experience harassment? Establish processes and best practice – make sure everyone understands.

“It’s Happening Now” Action Plan

- **Don’t feed the trolls:** Make sure all staff understand the risks of engaging with online harassment directly. Report content to platforms where it breaches their terms of service.
- **Protect your people:** Is there any risk of offline spillover? Identify how immediate the risk is and take immediate safety measures if necessary.
- **Document and escalate:** If you feel a crime has been committed, make sure you document evidence and escalate accordingly.

“Who to call” Contact Directory

- Call the police if there is an immediate danger to life, there is violence or threats of violence, the crime is still in progress or the suspect is still at the scene. You can use online police reporting portals for non-emergency crimes.
- Contact the Wales Hate Support Centre if you think a hate crime has been committed: reporthate.victimsupport.org.uk
- Use the CALL Mental Health Helpline for Wales for emotional or mental health support: **0800 132 737**.
- Contact Citizens Advice for free advice on legal matters: citizensadvice.org.uk/wales

PART 1

Understanding the threat landscape

Social media platforms are increasingly being used to intimidate or harass individuals and organisations who are supporting inclusion and equality in Wales. Targeting can be traumatic, interrupt the work of organisations and put staff and service users at risk. Although most intimidation and threats do not move from the online to offline sphere, the damage can still be significant.

While concerns about harassment must be taken seriously, it remains essential that organisations – particularly those receiving public funding – are subject to appropriate transparency and scrutiny to maintain trust and accountability. This practical guide seeks to help organisations to identify the difference between legitimate scrutiny and harassment and consider how they can protect themselves where necessary.

How campaigns against organisations typically develop

There have been several examples of organisations and individuals being targeted and harassed while delivering community services across Wales. These incidents have shared some common characteristics:

- Incidents often **start online** after an organisation posts a message on social media highlighting a piece of work, such as an event, educational project, or professional training to promote equality, diversity, inclusion and human rights. Historical posts about these subjects are increasingly also being targeted.
- Users will attempt to create outrage (engagement) by misrepresenting the organisation's work or posts. Exaggeration and distortion of misinformation is used to encourage a '**pile on**' of negative comments targeting an organisation or staff.
- Attempts may be made by malicious actors to 'dox' staff by releasing or highlighting **personally identifiable information** – such as full names, job titles, office locations, personal telephone numbers, social media accounts and email addresses. 'Doxing' is when a user collects information with the intention of embarrassing or intimidating an individual. This information is often obtained and harvested from public sources such as open personal social media accounts and organisational websites.
- In some cases, the online activity results in **offline harassment**. This could include: individuals or groups visiting the premises of an organisation to intimidate, interview or film, acts of vandalism, the receipt of malicious correspondence, or physical abuse.

What counts as harassment vs. free speech

Freedom of speech in the UK is protected under Article 10 of the Human Rights Act 1998. It protects everybody's right to hold personal opinions and to express them freely without government interference. This is a fundamental human right which facilitates an open and fair democratic society. It should enable people to agree or disagree with those with power and influence, and to do so without fear of reprisal. Freedom of speech also allows individuals to express unpopular or offensive views. It is important to say that critical or upsetting statements about the work of your organisation may well be protected by Article 10 and so be lawful, no matter how unpleasant or upsetting it may be.

However, freedom of speech does not protect unlawful behaviour such as threats of violence, hate speech and harassment, whether online or otherwise.

In England and Wales there are a range of Acts of Parliament containing offences which may be relevant:

- Hate crime protections can apply online or otherwise and are included in the Crime and Disorder Act 1998 and the Sentencing Act 2020.
- Incitement to hatred offences (on the basis of race, religion or sexual orientation) are set out in the Public Order Act 1986.
- Malicious communication offences are outlined in the Malicious Communications Act 1988, the Communications Act 2003 and the Online Safety Act 2023.
- Offences relating to harassment and stalking are included in the Protection from Harassment Act 1997.
- Incitement to terrorism offences are captured in the Terrorism Act 2006.
- Spreading disinformation which may cause non-trivial harm is prohibited by the Online Safety Act 2023.

Whether an incident has crossed the line from unpleasant but permitted freedom of expression into unlawful activity can be difficult to ascertain. If you feel this line has been crossed, we recommend that you report the incident to the police.

When is it misinformation, disinformation or something else?

It can be difficult to separate legitimate criticism or beliefs about the work of your organisation vs. spreading of misinformation. Misinformation is often used as a catch-all term for the spreading of information which is false and may cause harm. However, there are different forms of this practice which need to be understood.

Misinformation refers to verifiably false information that is shared without an intent to mislead. The effects of this can still be harmful.

Disinformation refers to verifiably false information that is shared with an intent to deceive and mislead. This can often have harmful consequences.

Malinformation refers to information which is sometimes true, or partially true, which is used in such a way that it has similar effects to disinformation. For example, facts or statistics can be taken out of context to support false or exaggerated claims. Malinformation is a deliberate attempt to mislead by distorting truthful information.

Alternatively, some of the claims people may be making about your organisation may be edited or framed to support their views or beliefs. There may be no deliberate attempt to mislead anyone.

It can be very difficult to prove the motive behind the actions of those criticising your organisation. Motives may or may not be malicious.

PART 2

Prevention strategies

Having discussed the nature of the threat and defined the potential offences and motivations of those targeting your organisation, we move our focus to how you can best prepare and prevent some of this happening.

Digital Security Audit tool

The Digital Security Audit Template is designed to help you assess how your online footprint is potentially leaving you vulnerable – and how urgently attention is needed. The tool will help you to use your own judgement about whether your footprint needs attention.

Before completing the Digital Security Audit Template below, we would recommend you visit the National Cyber Security Centre’s Cyber Essentials website. This website provides important user-friendly guidance for many types of organisation – [Cyber Essentials – NCSC.GOV.UK](#)

Digital security assessment

Footprint area	Category	Question to consider	Needs attention?
Web and online presence	Organisation address	Is it essential this information is made public? Could a PO Box be used instead?	
	Staff names	Is it necessary to publish the personal names of employees? Can you use job titles instead?	
	Contact details	Do you have a general enquiries email address which could be used for external enquiries, rather than a personal email? Email addresses can be harvested for phishing attacks.	
	Staff photos	Is providing staff photos necessary? Do staff consent to these images being public? Remember, images can be searched online to find matching images on social media profiles or elsewhere.	
	Event locations	Do you need to publish exact addresses publicly online before events? If so, could this be withheld until just prior to the event taking place?	
	Website content	Consider reviewing your web presence for information which could be deliberately or unintentionally misconstrued. Use clear language when describing the organisation’s work to avoid misunderstandings. Keep content up to date in response to the changing landscape. Remove historical resources or news stories if no longer relevant or useful to your audience.	

Footprint area	Category	Question to consider	Needs attention?
Social media accounts	Profile information	Does your organisational account reveal any information in the bio which could be useful to attackers? Are you able to lock your social media accounts to followers or those you want to see your posts?	
	Location data	Are you sharing real-time location data in your posts? Remember that some geotag data could be retained when images are posted.	
	Staff personal accounts	Have staff been asked not to reveal their employer in their social media bios? Has the organisation conducted an audit of whether an attacker might be able to find these details online? Have you considered historical posts (determined individuals will comb historical profiles and present information as if it is new)?	

Protect UK has developed the very useful ‘Blue Book: A Guide to Personal Security’, which includes sections on [IT security and online communications](#) and [Publicity and the Media](#), which you may find useful to consider.

Social media platform help and settings

Remember that social media platforms will normally provide a range of help pages to help you set up two factor authentication, review privacy settings, restrict page access, tagging or messaging, ban or block accounts and help you understand community guidelines or terms of service. Some of the more commonly used platform help pages are linked below but other platforms will have their own pages:

Bluesky [Community Guidelines – Bluesky](#)

Facebook [Facebook Help Centre](#)

Instagram [Help Center](#)

LinkedIn [LinkedIn Help](#)

Snapchat [Snapchat Support](#)

Tiktok <https://support.tiktok.com/>

WhatsApp <https://faq.whatsapp.com/>

X [Help Center](#)

Youtube [YouTube Help](#)

Social media companies are unlikely to take action against accounts or content where this does not breach their Terms of Service or Community Guidelines. All platforms will include these on their platform and organisations should consider these to understand how to raise matters with social media platforms.

Event planning security considerations – Questions to ask

When planning an in-person or online event, it helps to think through security early. Use these questions as a checklist to make sure risks are spotted and managed before the day.

Stage	Area	Questions to Ask
Before the Event	Venue & Access	- Who controls entry/exit/meeting lobby? - Do attendees need tickets or a guest list to manage disruptors? - Are you withholding venue details/meeting links until just before the event? - If online, do you require a meeting pass code? Only share the joining link with participants through direct communication methods (not advertised on the open web). - How do staff check attendees on arrival?
	Staff & Volunteers	- Does everyone know their roles if something goes wrong? - Who is the named security lead? - Are security guards required? If not, what other mitigations are in place to manage disorder and record evidence? - Have staff been advised not to speak to unexpected third parties who appear to film the event and interactions with your organisation?
	Technology & Online Safety	- Are you using organisational accounts (not personal ones)? - Do you have the ability to mute/block participants? - Are these controls limited to the call organiser? - Are participants restricted from sharing their screen?
	Data Protection	- How are you storing attendee information (sign-in sheets, registration forms)? - Who is responsible for handling/deleting it afterwards?
During the Event	Access & Monitoring	- Who is monitoring entry, chat, or audience behaviour? - Is there a clear and effective way for attendees to flag problems?
	Communications	- Who is the single point of contact for urgent issues? - Do staff know how to report harassment or suspicious behaviour quickly?
	Crisis Planning	- What will you do if trolling, harassment, or protest happens? - Who has authority to pause/stop the event if needed? - How would you log incidents (screenshots, notes, photos, police reports)?
After the Event	Incident Review	- Did anything happen that needs to be followed up (complaints, trolling, security breaches)? - Who will lead on writing up what worked/what didn't?
	Staff/Volunteer Support	- Is there a quick debrief so staff/volunteers can share concerns? - Do any individuals need follow-up support after dealing with difficult situations?
	External Follow-Up	- Do you need to notify the venue, police, or platform provider about incidents? - Should you update future plans based on what you learned?

Protect UK has developed the very useful ‘Blue Book: A Guide to Personal Security’, which includes sections on [Incident Procedures](#) and [Physical Threats](#), which you may find useful to consider.

Remember to also consider the risks associated with lone-working, including at other organisations’ events. Ensure your organisation has a lone-working policy with appropriate safeguards and processes which are communicated regularly to staff. For instance, establishing protocols for checking in and checking out with managers when travelling or working alone is good practice.

Staff training basics – Tips about what everyone should know

Employers have legal duties to try to keep their staff safe at work. While online abuse may not always be preventable, there are steps which can be taken to help all staff feel more confident and supported about staying safe online and knowing what to do if harassment happens. Organisations should always take advice about their individual responsibilities and circumstances.

Area	Key Guidelines
Passwords & Access	• Always use strong, unique passwords for work accounts. • Never share login details, even with trusted colleagues. • Use two-factor authentication wherever possible.
Personal vs Work Accounts	• Do not manage organisational pages from personal profiles if avoidable. • Keep personal opinions on your own account – avoid blurring lines. • Never reveal who you work for or where you work on personal accounts.
Recognising Harassment	• Trolls want a reaction – do not engage unless absolutely necessary and never from personal accounts. • Escalate abusive messages/comments instead of dealing with them alone. • Remember it’s not about you; it’s about the organisation being targeted and the beliefs of the attacker.
Reporting & Escalation	• Know the internal process: who to tell if you see abuse online. • We encourage you to report any abuse you receive. • Use platform tools to mute, block, or report – don’t leave it sitting visible. • Keep screenshots or logs if something is serious. • Ensure staff training includes these procedures and lone-working processes.
Privacy & Safety	• Check your own privacy settings on social media – limit what strangers can see. • Don’t share personal contact info on organisational channels. • Think twice before posting location details in real time.
Wellbeing	• If online abuse is affecting you, let a manager know – support should be available. • No one should be expected to face harassment alone. • Take breaks from monitoring if it’s overwhelming.

PART 3

Incident response procedures

Immediate response actions – What to do if targeted

The personal views of those working in the third sector are likely to align closely with the aims of the organisation they represent. When online harassment or related real-world incidents occur, it is likely to feel like a direct attack on the employee or the service users they support. A natural instinct is to defend your record or feel there is a mass of hostile accounts targeting you. However, the following clear immediate steps can help contain the situation, protect staff, and manage communications effectively.

Step	Key Actions
Identify and Contain	• Assign a single point person to coordinate the response for the organisation. • Determine the nature and scope of the incident online and any offline spillover. Who is at risk and how present is the danger? • Apply immediate safety measures: restrict access to premises, IT or social media accounts; remove or block content if necessary; mute/block abusive accounts. • Inform staff who need to know, particularly those directly affected. Provide details of existing staff well-being support. • Are new security measures required (e.g. reset passwords; emergency alert lanyards; new check-in procedures)? • Start collecting evidence if you believe a crime may have been committed.
Escalate Internally	• Alert senior staff and any other key staff/Trustees. • Record all activity: screenshots, URLs, timestamps etc. • Decide if external support is needed (social media platform reporting teams, police, venue security). • Remind staff about response procedures. • Brief staff on appropriate conduct: do not engage with trolls or in-person abusers, stick to official communication channels, report suspicious activity. • Involve your Trustees for awareness and support.

Step	Key Actions
Consider External Communication	• Consider reporting to the Charity Commission as a serious incident. • Assess whether a public response is appropriate. If a response is made, most successful counter-narrative work happens within the first couple of hours. • Prioritise your overall comms response based on likelihood of public harm – focus on whether it threatens safety. • Consider your audience closely – you may need different messages to be sent through different channels for each audience. • A holding statement should aim to: » Establish what is known of the situation. Use clear, factual information rather than repeating false claims. Keep it concise. » Provide messages which can reassure stakeholders, commit to regular and reliable updates. Provide a clear indication of next updates or review points. Example: “We will provide a full update tomorrow once the review is complete.” » Avoid using the terms ‘misinformation’ or ‘disinformation’ unless you are sure that is what it is. » Avoid making promises you cannot keep. » Explain what the organisation has done to manage the incident. Include actions taken to reduce the harm. » Outline any steps staff, trustees or service users should take to stay safe. Examples: “Do not engage with the trolls,” “Report any suspicious activity to your line manager,” “Follow official channels for updates.” See ‘Part 4: communication strategies’ for further detail.
Monitor and Support	• Continue monitoring online and offline developments. • Provide support to affected staff (check-ins, access to wellbeing resources). • Consider how harassment could disproportionately affect staff or service users from marginalised backgrounds, and how different levels of support may be required. • Review logs and plan next steps for containment or further communication. • Schedule a debrief to review the incident and inform recovery/resilience planning. • Consider the lessons learnt from the situation and review and update internal practices in response.

Documentation Templates – How to record incidents effectively

Fill this out as soon as possible after an incident. Keep it factual and concise. Save screenshots or other evidence alongside this form.

Field	Example/Guidance
Date & Time of Incident	When did the incident start and/or when was it noticed?
Platform/ Location	E.g., Twitter/X, Facebook page, Instagram, LinkedIn, in-person venue.
Description of Incident	Brief factual summary: what happened, what content appeared, who was involved.
Immediate Actions Taken	E.g., content removed, accounts muted/blocked, staff informed.
Staff Involved/ Notified	Who saw it, who responded, who escalated?
External Support Contacted	E.g., platform reporting, police, venue security (if applicable).
Evidence	Screenshots, links, photos, videos – attach or reference here.
Follow-Up Actions Needed	Next steps: further communication, monitoring, debrief, recovery plan reference.
Additional Notes	Any other relevant context or observations.

PART 4

Communication strategies

Communication strategies is a critical aspect to consider as part of your response. However, there are things for you to understand about how social media platforms work, realities about user behaviour, how messages resonate with the public, and how certain types of response can exacerbate the issues you face.

Social media platform dynamics and user behaviour

Algorithms can shape the effectiveness of communication strategies. They prioritise content similar to what users previously engaged with or what is trending among similar audiences. Divisive or overly simplified content often attracts high engagement, and on platforms like X, creators are financially rewarded for such engagement. This environment can make mis-, dis-, and malinformation more potent. Engagement spreads content further, even when users oppose it. Direct rebuttals can backfire by generating new content for distortion, which is why we generally advise against ‘feeding the trolls’.

Algorithmic bias toward divisive content is amplified by reduced moderation. Users chasing engagement know bans on many platforms are now less likely, leaving organisations with limited platform support from harassment. Attempts to counter misinformation with facts and links rarely succeed: platforms like X and Meta may downgrade posts containing hyperlinks, whilst evidence suggests most users do not read articles they share – studies suggest up to 75% of shared news is never clicked by the poster.

Finally, facts seldom change minds when they conflict with deeply held views. Telling someone they are wrong rarely works. Instead, framing your message to align with their values is far more effective. Recognising these dynamics is essential for building a communication strategy which resonates and avoids reinforcing harmful cycles.

Moral Foundations Theory

Moral Foundations Theory suggests people judge what is right and wrong based upon six core ‘foundations’:

1. **Care/Harm** – Compassion and protection from suffering.
2. **Fairness/Cheating** – Justice, equality and fair treatment.
3. **Loyalty/Betrayal** – Standing with your group or community.
4. **Authority/Subversion** – Respect for tradition and leadership.
5. **Sanctity/Degradation** – Purity, sacredness, and avoiding contamination.
6. **Liberty/Oppression** – Freedom from domination or control.

Charities often appeal to Care and Fairness when countering misinformation, hate, or harassment. These messages resonate with natural supporters, but different audiences respond to messages framed across all foundations. To succeed, tailor your communications to align with the whole audience's values.

Your organisation may rarely frame responses around defending freedoms, avoiding degradation, or citing voices by other audiences. Yet doing so can help craft messages which engage without alienating those influenced by mis/dis/malinformation.

Alternative narrative rather than counter narrative

Before deciding to counter claims, consider whether the claims are likely to cause real-world harm and the scale of engagement with false narratives. Responding can amplify awareness and lead traditional media to frame the issue as a balanced dispute. Denying claims the oxygen of publicity may be wise.

However, not responding may be unacceptable for your organisation. If correcting claims, use spokespeople/individuals who are more likely to be trusted by the audience you wish to persuade. If the audience has been primed to distrust your organisation, they are unlikely to give your message a fair hearing directly. Finally, anticipate how those spreading falsehoods will react. Draft your statement to pre-empt likely counterclaims without escalating the situation further.

Proactive partnerships

Another important aspect of building a response is developing and maintaining a proactive partnership of like-minded organisations who can provide solidarity when any of your organisations are targeted. Building a partnership can help you to coordinate messaging, develop a rapid response network, and share learning and knowledge about tools and approaches which have worked.

Building a partnership which can publicly talk about an alternative narrative will help in demonstrating to the public that there is support for the work your organisation does. It will help you to demonstrate that the false claims and your response should not necessarily be considered to have equivalent weight. The wider and more varied partnerships you are able to build, the more likely it will be clear that the abuser is in a minority.

PART 5

Support directory

If your organisation is targeted, remember that you are not alone. This section highlights various services and approaches which may be available to support you.

Police

Perpetrators of hate and harassment will very likely hide behind anonymous accounts and may not be easily identified. This makes them feel as if they can say things that they would never ever consider saying face-to-face. Regardless of whether a perpetrator is anonymous or not, some situations may escalate to the point where police involvement is necessary.

It is vital that you call the police via 999 in an emergency:

- When there is an immediate danger to life.
- When someone is violent or threatening violence.
- When a crime is in progress, such as damage to property.
- When the suspect is still at the scene.

If you've witnessed or been the victim of crime that is not an emergency, you can report it online via the links below:

- [North Wales Police](#)
- [Dyfed Powys Police](#)
- [Gwent Police](#)
- [South Wales Police](#)

Wales Hate Support Centre

A hate crime is any criminal behaviour which appears to be motivated by a hostility or prejudice, or includes words or behaviour that show hostility, based on a person's perceived:

- race
- religion
- sexual orientation
- transgender identity
- disability.

A hate crime can include verbal abuse, intimidation, threats, harassment, assault and bullying, as well as damage to property. Hate crime can take place both in person and online.

The Wales Hate Support Centre, run by Victim Support Cymru, offers independent and confidential support and advocacy to victims and witnesses of hate crimes in Wales. Not all cases will be able to proceed to court, but you will be offered support to help you deal with what has happened to you regardless. You can also report hate crime to the Wales Hate Support Centre if you don't feel confident reporting to the Police.

You can call the Wales Hate Support Centre for free and at any time on 0300 3031 982 or via e-mail Hate.CrimeWales@victimsupport.org.uk.

You can find out more by visiting their website: <https://reporthate.victimsupport.org.uk/>

Funders

Your funder may have established approaches to help targeted charities in these circumstances. Consider approaching them to seek support and notify them of the risks your organisation is encountering in delivering funded activities.

The Charity Commission

Charities are required to report serious incidents to the Charity Commission. This includes incidents which results in, or risks, significant harm to a charity's beneficiaries, staff, and volunteers, as well as an incident resulting in damage to a charity's property.

The Charity Commission will want to know what has happened, how the situation is being dealt with, and whether it has been reported to the police. Guidance on how to identify serious incidents, and where to report them, is available online.

The names of all charity trustees are displayed to the public on the charity register, unless a dispensation has been granted. In special circumstances, such as when a person or people are in physical or mental danger, it is possible to remove a trustee's name from the public charity register. This is known as granting a dispensation. You can make a request for dispensation directly to the [Charity Commission](#).

Social media Trust and Safety teams

In recent years many social media Trust and Safety teams have reduced the ways in which they will intervene to remove harmful content, block users, or provide identifiable details to Police. However, we would still advise all targeted individuals and charities to report harmful content, as this can still have a beneficial effect in some cases, and evidence steps you took to protect your organisation. Remember that action is unlikely to be taken where the platform Terms of Service have not been broken or where a crime has not been committed.

Regulators – Ofcom, Standards Commissioner etc

Another option for your organisation is to consider whether a regulatory body could be helpful in helping you to protect your organisation in future. For example, you may be able to provide evidence to Ofcom (or work with Welsh Government or another organisation to do so) as a means of helping them to enforce the Online Safety Act 2023.

Similarly, if your abuser is a politician they will be bound by a Code of Conduct overseen by a Standards Committee/Commissioner. Your organisation could appeal to the relevant body to ensure any breaches of that Code of Conduct are investigated.

If the account targeting you is fundraising but seemingly not properly incorporated, you could appeal to the Charity Commission or Companies House to investigate.

Wales Council for Voluntary Action/County Voluntary Council

The WCVA and your local CVC are established to provide the infrastructure supporting the third sector in Wales. They are keen to provide support to third sector organisations who have been targeted because of their work and may have useful guidance they can share to help you navigate the current challenging circumstances. In the past they have published statements of solidarity for targeted organisations.

Useful Contacts

[CALL Mental Health Helpline for Wales](#)

CALL offers emotional support and information/literature on mental health and related matters to the people of Wales.

[Citizen's Advice](#)

Free online advice on a range of subjects including law and courts.

[The Charity Commission for England and Wales](#)

The Charity Commission also produces guidance on Safeguarding and protecting people for charities and trustees – [Safeguarding and protecting people for charities and trustees – GOV.UK](#)

[National Protective Security Authority](#)

The National Protective Security Authority has produced guidance on social media Auditor activity for security personnel and general staff.

[Protect UK](#)

Protect UK provides free advice, guidance and learning to help organisations and communities understand protective security and improve their response to the risk of terrorism. Their guidance includes lots of helpful information and resources for sub-terrorism threats too.

Welsh Government

Unfortunately, the Welsh Government cannot investigate incidents of hate or harassment or get involved in criminal investigations.

Criminal justice is a reserved matter and therefore responsibility for policing sits with the UK Government. Although the Welsh Government works closely with Policing in Wales on areas of joint interest, Forces have autonomy over the operational decisions they make, and it would be inappropriate for the Welsh Government to comment on a reserved area of practice or intervene in individual cases.

However, the Welsh Government might be able to offer targeted support and encourage partnership working to assist and bolster the mitigation of tensions, as well as signposting affected individuals to relevant support and advocacy.

In some situations, Welsh Government is not best placed to speak publicly about ongoing community tensions. Doing so may unintentionally amplify any mis/dis/malinformation to a much wider audience, particularly when engaging via social media or traditional media.

If you have suggestions about how to improve this guide or responses to these challenges, please send them to: cohesion@gov.wales