

SAFETY PLANNING TOOLKIT

A practical guide for doing great work even
when things feel scary



CONTENTS



Introductions & author's note

2

Using this resource

4

Chapter 1: Understanding the problem

5

Chapter 2: Preparedness

15

Chapter 3: Planning

29

Chapter 4: Wellbeing

41

Chapter 5: In the moment

46





For many of us across different sectors, offering public comment or organising events comes with increasing risks related to disruption, harassment and silencing.

Groups are more organised in terms of their disruption activities, and are well aware of how platforms and events work to have maximum reach and impact. They do this with the aim of silencing others.

This toolkit was designed to support organisations and individuals to ensure their voices aren't silenced by attacks. While attacks are targeted against individuals and specific organisations, we know that a collective and systemic response is required. Our parallel work on the [#NoHarmware](#) campaign seeks to push for regulatory reform.

Until that happens, we know that our communities need support and tools to keep themselves as safe as possible as they continue to raise their voices on important issues. We hope you find this useful, and please do get in touch if there is anything that can be added to this toolkit.

Anjum Rahman
[Tahono.nz](#)

In today's activism environment, many people are facing threats, with ongoing reports of targeted attacks both online and offline. This is a serious human rights issue and risks a chilling effect on our society, preventing people from coming together to be heard, to participate and to drive positive change. These are core things I think we all agree are valuable in a healthy, thriving society.

While broader work is urgently required to address the root causes of these threats, this resource aims to provide you with practical support to navigate this environment. Whether taking action as an organisation, an individual, a small group, a big group or something else, this resource contains a wealth of knowledge, tips and suggestions that we hope you find helpful.

Lisa Woods
[Amnesty.org.nz](#)



AUTHOR'S NOTE



It's not a coincidence that the organisations and initiatives best placed to counter false information and polarisation are often the primary targets of harassment campaigns.

In the last few years, and on an ever-increasing number of topics, public engagement has become a complex and often frightening space to navigate.

As a longtime communicator, I'm honoured to have supported many organisations through an increasingly challenging 'new normal'. However, I want to be clear: this shouldn't be normal at all.

We should *never* accept that public engagement comes with an inherent risk of harm, or ignore how this disproportionately impacts already marginalised people and communities.

However, when profit-driven technologies are outpacing regulation and governments repeatedly fail to mitigate the harms caused, it falls to communities and civil society to look after each other. Thankfully, in Aotearoa, we are good at doing just that.

The work of community building and sharing skills and resources is precisely what reactionary movements fear. But that makes it part of the solution.

I hope that this toolkit helps you stay clear-eyed and equipped to keep doing your important work, whatever that may be, as safely and sustainably as possible.

Ngā kotahitanga,

Nicole Skews-Poole
Anchordown.nz

USING THIS RESOURCE

This toolkit unpacks the growing issue of online harm aimed at individuals and organisations. It's designed to provide information, ideas and resources to help you feel empowered to do important work — even in a challenging environment.

It's important to note that this toolkit isn't intended to be a comprehensive guide for all considerations, circumstances and requirements. Instead, it zooms in on the issue of targeted harassment and false information spread with the help of technology.

Not every approach will be right for every situation, so take the ideas that feel most useful and relevant for you.



TERMINOLOGY

This resource uses terms like 'actions' or 'events' as catch-alls for anything you do that engages people. This might include:

- * Maintaining an online presence that shares opinions and expertise.
- * Offering commentary in response to media enquiries or through articles and opinion pieces.
- * Holding meetings, conferences and panels (online or in person).
- * Launching campaigns, resources and reports.

We also use 'harassment' and 'online harm' as catch-all terms for things such as:

- * Using technology to knowingly spread false information.
- * Using digital platforms to direct harassment — including threats or repeated unwanted messages — towards (or about) individuals and organisations.
- * Sharing private information online (doxxing).

[illegible]

KEY POINTS FROM THIS CHAPTER

- * Networks of people regularly engage in harassment campaigns targeting individuals and organisations in Aotearoa. These groups use a range of digital tools to inflate their size, reach and impact.
- * These networks can give their members a sense of purpose and action, while skewing the information people are exposed to. This can lead to increasingly extreme beliefs and behaviours.
- * The themes and ideas promoted in these groups often exploit existing biases and target people and communities who already experience marginalisation.
- * Online actions have offline consequences. These groups aim to frighten people into silence and narrow what ideas and views can be expressed without fear of harassment.
- * Responding to harm and harassment can be time-consuming, but being informed and prepared makes it easier to keep doing important work.
- * Your work matters — especially in this environment. Events and trusted sources can help prevent polarisation and provide a counter to false information.

In recent years, Aotearoa New Zealand has witnessed the growth of online networks promoting increasingly extreme ideas. Many of these groups were formed or accelerated during the COVID-19 pandemic. These groups use technology like social media to spread false information and organise harassment campaigns against chosen targets.

Aotearoa is not alone, and there are local and global efforts to understand and counter this harm. However, the problem continues to grow while lawmakers and communities work to keep pace with the complex legal, technological and social challenges involved.

THE APPEAL OF THE RABBITHOLE

Given how small and interconnected Aotearoa is, you may know someone who has 'gone down the rabbit hole' in recent years.

It can be difficult to understand how people come to believe extreme or upsetting ideas, and even experts are grappling with why false information has drawn in so many people, and how best to mitigate it.

Some of what's appeals to people about these groups are things like:

- * A sense of belonging. even within communities built around harmful beliefs.
- * Feeling purposeful and active in defence of shared values.
- * The excitement of discovering "new" information (which is often recycled beliefs being presented in different ways).
- * Being offered convincing — but false — explanations for complex global and personal problems, often by blaming particular groups.

THEMES & TARGETS

Effective lies often contain an element of truth. A common theme in false information is the claim that governments, supported by powerful “in-groups”, are deceiving the public on a large scale.

However, rather than confront genuine examples of corruption and abuses of power, some groups have obsessively organised around an increasingly extreme set of beliefs.

An example of this is the false belief that the COVID-19 pandemic was fake and involved mass deaths caused by vaccine harms, which is being covered up by groups ranging from your local healthcare provider through to leadership of the United Nations.

Other narratives exploit existing prejudices and target marginalised communities by spreading claims such as:

Honouring the Treaty of Waitangi will take away the rights of non-Māori as part of a conspiracy between the government and a perceived group of ‘elites’.

Transgender and non-binary people are a danger to children.

The growth of immigration into New Zealand and other countries will result in the ‘replacement’ of white people.

Women’s rights have gone too far, and women are failing in their traditional roles as mothers and caretakers.

Moves to be more environmentally friendly, especially in infrastructure and transport, are secretly a way to take away people’s private property.

FALSEHOODS

SUPERSPREADERS

Unfortunately, powerful people with platforms, like reporters and politicians, sometimes act to further the spread of false information, both inadvertently and on purpose.

For those in the media, it can be hard to counter false information when newsrooms cut jobs like editors and fact-checkers while expecting reporters to publish large volumes of eye-catching stories.

Some individual commentators are platformed by media outlets to promote the idea that they're showcasing 'both sides' of an issue. This position can be dangerous when commentators are given the same level of platforming as scientists, scholars and subject-matter-experts.

In the political sphere, politicians have often engaged in false or misleading information when it could be perceived to benefit them. However, this problem has escalated in recent years, with some local politicians promoting increasingly polarising ideas and refuting evidence-based decision-making.

This bad behaviour works to further people's distrust in politicians and the media, and can drive people to disconnect from traditional sources of information, becoming more susceptible to information sources that are even less credible.



ONLINE VERSUS OFFLINE

There is no longer a meaningful divide between "online" and "offline" spaces. While parts of the internet have always hosted harmful content, this is no longer confined to obscure forums, and technology can be used to inflate its reach.

Information shared online shapes real-world actions, for better and worse. This means that when online spaces become hostile, the impact doesn't stay there.

DISTRUST & VIOLENCE

There are many communities in Aotearoa that have every reason to distrust the government. It's also often useful for democratic societies not to automatically accept what people in power say.

However, one of the challenges of the current environment is a growing distrust towards a growing number of democratic institutions, organisations and their staff, alongside the normalisation of 'holding people to account' through threats and harassment.



During the Parliament Occupation in early 2022, gallows and nooses were erected in the occupation encampment, and protestors called for politicians, media and public servants to have citizen-led trials and executions.

More recently, libraries around the country have experienced threats and direct violence in response to events celebrating the LGBTQ community.

RIGHT FEELINGS, WRONG FACTS

In a global environment of entrenched inequality, conflict and environmental harm, many people are understandably frightened, angry and feel that our current systems are failing us. However, reactionary groups rarely engage meaningfully with genuine examples of power and harm, and often rely on inconsistencies or shifting goalposts. For example:

- * **People who are 'anti-elite' and believe politics is inherently corrupt may rally behind tenured politicians.**
- * **Distrust of pharmaceutical companies may be redirected towards transgender people seeking gender-affirming care.**
- * **Public servants of all levels are deemed appropriate targets of people's anger and distrust.**

USING TECHNOLOGY FOR HARM

Networks that spread false information use a variety of digital tools to create content, grow their reach and coordinate harassment. Here's an overview of their tools and approaches.

Group chats & channels

These messaging and broadcast platforms range from moderated and commonly used spaces like WhatsApp to completely unmoderated platforms such as Telegram.

'Alternative' media

Streaming and broadcast platforms have been used to create parallel media ecosystems which help the spread of false information and aid in harassment campaigns. These spaces and their figureheads can gain legitimacy when public figures agree to participate, and their platforms often seek to evade normal media regulations and standards.

Artificial intelligence & synthetic tech

These networks commonly use AI in many ways, most of which can be summed up as quickly and easily generating increasingly convincing content. This includes things like deepfakes and bots that mimic real users to artificially amplify false information.

Mainstream social media platforms

Facebook, Instagram, LinkedIn and other common platforms are used to research targets and spread harassment or false information. Platforms like X (formerly Twitter), along with purpose-built unregulated spaces, are hosting increasingly extreme content with limited moderation.

DDOS attacks

A Distributed Denial of Service Attack is when an attacker coordinates many devices to make so many requests that they overwhelm a web server or other online service, to the point where it can't respond.

THE TIME & COST OF SAFETY PLANNING

It's understandable to feel wary of the risks posed by online harm, or daunted by the amount of work needed to respond. It's important to know that this is by design – bad actors benefit from people feeling less free to express opposing views.

This is what's called a 'chilling' or 'silencing effect', and it lands disproportionately on people and communities who already experience marginalisation, and smaller organisations who have fewer resources to invest in prevention and response.

The purpose of safety planning is to have a clear-eyed awareness of the risks involved, so that you can make informed decisions about taking those risks. If you or your organisation doesn't feel equipped to manage potential harassment right now, it's okay to pause.

It's important to remember that harassment can occur even when you haven't actively engaged.

This makes safety planning worthwhile, even if you carefully pick your battles. It helps you feel informed and prepared, even if you never need to use it.





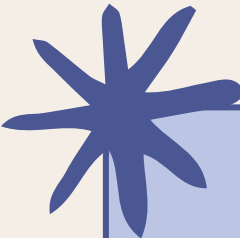
BRINGING PEOPLE TOGETHER, ESPECIALLY WHEN IT'S HARD

You don't have to do this work alone. Given how widespread this issue has become, you should consider reaching out to allied organisations that are likely to be considering similar issues and risks. Keep an eye out for opportunities to collaborate and build shared approaches within your sector or your community. You can also reach out to organisations dedicated to dealing with online harm.

Even though public engagement comes with increasing challenges, it's critical to stay grounded in the value and importance of your work. Social polarisation is often caused by disconnection and loneliness, so holding events and sharing information can be vital preventions against this disconnect.

Events and information sharing are also powerful ways to respond to current challenges and bring people together with shared purpose. Similarly, storytelling and good information can be a way to counter false information before it takes root and offer trusted sources for the general public to rely on.





RESOURCES

- * [Typology of online harms | World Economic Forum](#)
 - * [Online abuse and harassment | Netsafe](#)
 - * [What is online abuse? | PEN](#)
 - * [Online harm and why it matters - Transparency Intl NZ](#)
 - * [Technology and online platforms | Classification Office](#)
 - * [The Conspiracy Theory Handbook | Skeptical Science](#)
 - * [Understanding the NZ Online Extremist Ecosystem | ISD](#)
 - * [Freedom-to-Read Toolkit | LIANZA](#)
 - * [The Role of Community Building in Depolarisation | DepolarWise](#)
 - * [Social cohesion and societal polarisation | UoA](#)
 - * [In-person events fosters social connections | UoG](#)
 - * [Storytelling as a Tactic for Correcting Misinformation | SPSP](#)
 - * [Social Cohesion in New Zealand 2026 | Helen Clark Foundation](#)
- 

CHAPTER TWO: PREPAREDNESS





KEY POINTS FROM THIS CHAPTER

- * Take the time to clarify the purpose of your event or action, and decide on realistic measures of success.
- * Draw on your existing skills and experience, and make sure people have clear roles and responsibilities.
- * Where possible, identify and build relationships with people whom you might need to call on for support in the event of an incident.
- * Make sure you review and improve your digital security - both personal and organisational. Think about ways to keep friends and whanau safe, as they can be both targets and access points for bad actors.
- * Ensure you understand your organisation's risk environment, and consider how you will monitor your risks and use that to inform your decision-making.





PURPOSE & SUCCESS

The most important part of planning for activities is getting clear on **why** you're doing this and what your goals are. Here are some things to consider:

Who is your audience?

Who are your stakeholders, or the people who are impacted by your action? What do you want them to know, feel or do based on your action? Who are the groups that you should put your time and resources into reaching?

Who is *not* your audience?

What groups or individuals are you *not* trying to engage with? Who do you expect might oppose you, and to what extent?

Why are you doing this?

What do your audience need? How can your action stay focused on your audience, even if other groups weigh in?

What are your goals?

What does a successful action look like? How will you assess or measure this?

Measuring success should be simple and realistic. In today's environment, Success does not mean universal agreement and bad-faith responses are likely to occur. If you expect that possibility, you can plan for it without losing focus on your audience.

Genuine disagreement

It's important to leave space for genuine disagreement and challenge. A good measure of this is whether the criticism is coming from people who have felt overlooked in the past, or from people who are pushing you to consider whether you're upholding unjust power structures.

Good faith-disagreement isn't always polite, but it is never threatening or violent. Consider talking with your team about how you might define good faith versus bad faith debate for the context of your event or action.



EVENT BASICS

For any events, major pieces of commentary, campaign launches or similar public-focused actions, it's important to have basic information planned out and readily available. This should include:

- * A timeline of planned engagements or events.
- * A specific run sheet for each event (online or offline).
- * Venue safety considerations for in-person events (e.g. housekeeping and emergency procedures).
- * Key roles, responsibilities and their contact information.
- * Emergency contacts, e.g. the people involved in safety planning.
- * Relevant plans that you develop using the next sections of this toolkit.



KEY ROLES & RESPONSIBILITIES

Planning for actions requires thinking about key people and the roles they will play. Not every role is required for every action, but common roles to consider are:

Facilitators & MCs

For many events and meetings, it's important to ensure there's someone responsible for sharing information to your audience (like setting a kaupapa for your event, introducing speakers, housekeeping, etc.). They should help manage any audience engagement while ensuring your event stays on time and on agenda.

It's especially helpful if people in this role feel comfortable de-escalating tensions and dealing with potential disruption. It can be worth investing in de-escalation training for people frequently holding these roles.

Spokespeople & media liaisons

Decide who represents your organisation to the public. These people should have all the information they need to feel confident and supported to be the face of your event or action.

Monitors & moderators

Ensure that you have dedicated people to keep an eye on the online sentiment ahead of, during, and after your event. These people should have clear ways to report any issues they find. It's important to support and resource your moderators, as these are the people who are asked to field harmful content on behalf of your organisation. They are an important, valuable resource in safety planning.





Greeters & crowd management

For in-person events, it's helpful to have someone greet people as they arrive and keep an eye on the tone and mood of the audience. They should be able to communicate easily with other organisers throughout the event if they sense there may be disruption. Sometimes this role might involve helping facilitate audience questions.

Safety reps

Anyone who has a role in responding to safety concerns before, during and after your action should be identified and kept across your plans and considerations. For example, workplace health and safety reps.



Drawing on your skills

Your organisation or wider community will already contain helpful knowledge and experience. It can be useful to do a stocktake of the skills and experience shared through your organisation and community, and work to fill any priority gaps you identify.

For example, if you're holding an event that requires crowd control, which groups within your community or your sector have held large or contested events before? Can you ask for their help, or collaborate with them?

RELATIONSHIP BUILDING

It's important to think about who you can ask for help if you experience targeted harassment or the coordinated spread of false information. Where possible, take the time to invest in building relationships before any incidents occur.

This might involve:

- * Establishing a named contact for local police (where appropriate).
- * Building a relationship with venue management before high-risk events and understanding their safety initiatives, e.g. asking how they screen staff who will be working at your event.
- * Identifying a legal contact in advance (even if informal).
- * Connecting with allied organisations that can publicly support you.

MEDIA ENGAGEMENT

Planning for media enquiries should be a key part of actions like launching a campaign or a report, publishing articles or commentary, and holding large-scale events.

It's reasonable to expect that media engagement will increase the reach and impact of your work. This exposure can be fantastic, but it also comes with increased risk of attention from bad actors. When you come to your scenario mapping, consider using media attention as a factor in your scenarios.



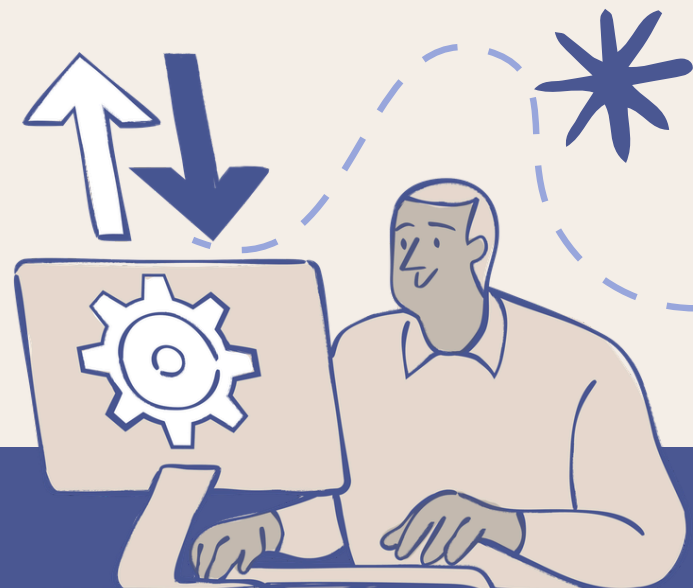
Attention from 'alternative media'

As briefly outlined on page 11, there are 'alternative media' ecosystems where figureheads position themselves as reporters, but are not subject to the same regulations and standards.

It's not recommended to respond to enquiries from channels that have a track record of platforming false information or allowing their comments sections to become vectors for harassment. This means you need to allocate time to research and assess enquiries from unknown media outlets.

Unfortunately, even if you ignore or reject invitations from these channels, they can still be a source of harassment. They can publish stories about you or your event, or host an interview with someone who opposes you. Sometimes, these channels might even post a story about you long after your event has passed.

This potential for harassment – even if you avoid engagement – is why it's important to have safety plans in place that can be enacted quickly regardless of the situation.



ONLINE EVENTS



If you're hosting an online event, make sure you're familiar with the tools you have available. Consider how to keep registration and event links secure, and how to utilise the moderation and sharing options in your platform of choice.

If you're planning to record and upload your event afterwards, it's important to know that recordings of online events can be circulated and used to facilitate harassment. This doesn't mean you shouldn't publish a video of your event, but it should be a consideration in your scenario mapping.

IN-PERSON EVENTS

Here are some key decisions, considerations and ideas for running an in-person event safely and smoothly:

- * Decide how your team will communicate with each other during your event. It's a good idea to have a group chat to share important information while your event is underway.
- * Ensure you have greeters or people to take registrations at the door. Keeping staff assigned to your venue's entrances and exits at all times during your event can help you manage access and increase your awareness of attendees' mood and movement.
- * Through your MC or facilitator, ensure all your attendees are aware of housekeeping, hazards, and evacuation points.
- * Consider how you will use microphones during your event. If you are taking open questions from the audience, it's important to have microphone runners who go to the audience members and hold - but not hand over - the mic so they can be heard. Keeping hold of the mic is an important way to mitigate any disruptive questions.
- * If you have high-profile speakers, ensure they are aware of how to enter and exit the venue safely. Keep them connected with your event organisers and aware of your prevention and response plans.



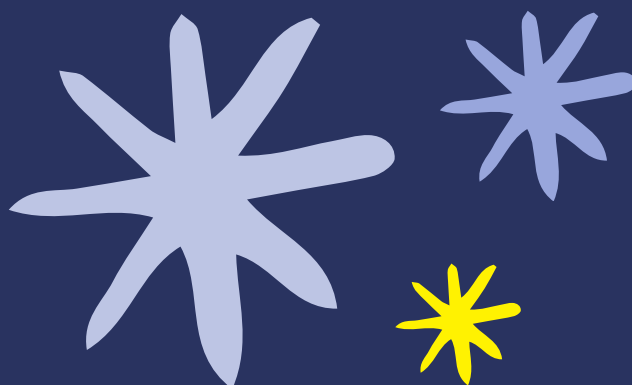
- * If you're expecting in-person disruption, or if your event has attracted protest, it's important to explain to your attendees what measures you're taking to ensure the event runs smoothly and safely.
- * Consider reaching out to a professional security firm to review your plans, and/or to provide a security guard at your event. If you're working with a large venue, they will likely have an existing relationship with security providers which they can connect you to.

FOR ALL EVENTS

It's important to set a kaupapa, tikanga or code of conduct for any event. This can be as simple as sharing the purpose of the meeting or action at the start, but events with greater risks of disruption or harassment should create and share expected standards of behaviour from attendees.

Let your audience know how best to engage. For example, you might use online platforms to moderate questions which the facilitator then asks, or you might allow online attendees to post questions in a shared chat.

You should have a confident facilitator or MC keeping things on time and on kaupapa. It's their job to share important information (like housekeeping and tikanga) and manage engagement from attendees.



RESOURCES

- * [Crowded places strategy | New Zealand Police](#)
- * [Facilitation guide | MBIE](#)
- * [Communicating via the media | CommunityNet Aotearoa](#)
- * [Example Code of Conduct | CommunityNet Aotearoa](#)
- * [A guide to meetings | CommunityNet Aotearoa](#)
- * [Managing risks at events | WorkSafe](#)

PERSONAL & DIGITAL SECURITY

It's important to take basic digital security measures for yourself and your organisation. This is particularly relevant for small organisations where boundaries blur between personal and professional.

Unfortunately, it is increasingly common for people's family members to become targets of harassment. Consider the visibility of your social media accounts and whether they can be used to identify your close friends and whanau.

Your family members may also need to consider the visibility of their online profiles, too.



You might also consider:

- * Auditing publicly available personal information for spokespeople and leadership.
- * Using PO boxes instead of home addresses for details on public records, and removing personal contact details from registers like WHOIS and company listings.
- * Considering the security of public wifi, sharing platforms and data exchange tools like Bluetooth.
- * Discussing family safety plans if whanau and friends are also targeted.

Website, information and domain security

If you think you might be subject to a DDOS attack (explained on page 11) you should consider using a hosting service that offers DDOS protection, or see what your existing provider offers. If not, it might be helpful to look into a content delivery network (CDN), like CloudFlare or Fastly. These services generally offer a free package that provides some protection, and you can upgrade if you need to. Consider having a backup of essential information stored somewhere else.

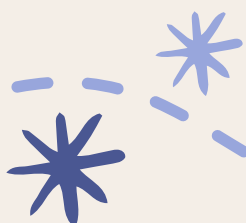


Malicious social media account takedowns

A common tactic from bad actors is to abuse the reporting features on social media platforms to get your account suspended. It can be slow and difficult to get an unfair suspension reversed, which is the intention of this malicious reporting.

One way to deal with this is to have other channels prepared in advance. This could include having backup or alternative accounts, with the same or other social media platforms, mentioned in your profile.

It's always useful to have a website you control, with your own domain name, even if it doesn't have much content. You can use it to provide alternative contact details, and to confirm which social media accounts are genuinely yours.



RESOURCES

- * [Keeping Yourself Safe | Health and Safety](#)
- * [Online Abuse and Harassment | Netsafe](#)
- * [Domain Lookup | Whois](#)
- * [Online Security Assessment Tool | Own Your Online](#)
- * [Digital Safety Snacks | PEN America](#)
- * [How To Stay Safe | LGNZ](#)
- * [Supporting Researchers | Science Media Centre](#)
- * [Resources | Researcher Support Consortium](#)
- * [Online Harassment Field Manual | PEN America](#)
- * [Digital Safety Kit | Stop Online Harm](#)
- * [Surveillance Self-Defence | EFF](#)
- * [Protect Your Organisation | NSSC](#)



UNDERSTANDING YOUR RISK ENVIRONMENT

A great place to begin when thinking about the risks you or your organisation face is to consider the themes and falsehoods we discussed on page 8 and where your work and expertise overlap with those themes.

Take a look at local and overseas organisations that are similar to yours, or individuals who have similar roles and expertise as you, and research their online presence to see what challenges they have encountered. You may want to consider monitoring specific digital platforms for keywords that are relevant to your work, or invest in software that can help you monitor the mood and sentiment of your online audiences.

For those responsible for monitoring and moderating your online channels, make sure you are aware of any helpful tools that can help you streamline your approach. For instance, there are a variety of free and paid tools that can help you mute or block certain keywords, and some platforms like Meta (Facebook) offer some built-in moderation tools that you can familiarise yourself with.



RESOURCES

- * [Social Media Monitor Toolkit | DRI](#)
- * [Monitoring and Evaluation | Campaign Toolkit](#)
- * [Social Media Moderation Tools | Social Factor](#)
- * [Online Content Moderation | MIT Sloan](#)
- * [A New Age of Social Media Moderation | CharityComms](#)



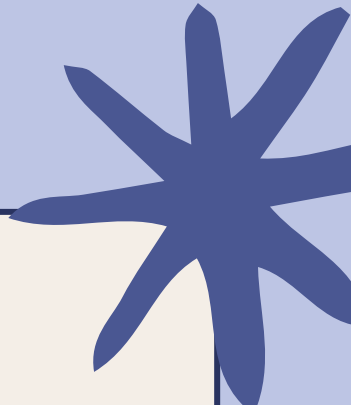
CHAPTER THREE:

PLANNING





KEY POINTS FROM THIS CHAPTER



Creating a safety plan can be as simple or as complex as your situation requires. A good start is to do some scenario mapping.



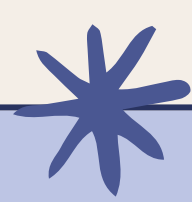
Use your scenarios to build out an escalation plan, and stay grounded in your people and purpose.



Consider how communications and key messaging can be used to mitigate and respond to false information.



Make sure you plan for what happens after your event, especially if an incident occurs.



The following sections offer approaches you can use to create a safety plan in response to risks posed by online harm. It's important to note that every event or project has wider health and safety obligations which we can't cover in this resource. Not every approach will be appropriate for every situation, so pick and choose what feels relevant and realistic for you or your organisation.

Remember that you can't control the behaviours of bad actors, and that you can't be expected to capture every possible scenario. Instead, the goals of safety planning should be to:

- * Help you and your organisation feel more aware of the risks you face.
- * Know what approaches you can take to prevent, mitigate and respond to those risks.
- * Clarify the actions you'll take in the event of an incident. This means that even if something scary or stressful happens, you're not adding to the stress by trying to make important decisions in the heat of the moment.



It's important to know that scenario mapping itself can be distressing – you're mapping out frightening scenarios that directly affect you and your organisation.

If you're finding this hard, consider staggering out your planning sessions or reaching out to an external facilitator with expertise in wellness.



SCENARIO MAPPING

Scenario mapping is a great way to plan ahead for a range of different challenges. The concept of 'safety planning' can sometimes feel vague and daunting, so scenario mapping is a great way to clarify what risks you are seeking to prevent or respond to.

Here's a basic mapping exercise you can do either by yourself or with a team. Take what you've learned in your risk environment research, or use past incidents you've experienced as starter scenarios.

EXERCISE

- 1** On a whiteboard, post-it notes or big piece of paper, write down a range of possible scenarios. Don't edit or spend too long thinking about each scenario at this point, just capture all the potential incidents you can think of.
- 2** Looking at all the possibilities you've captured, identify:
 - * The best-case scenario
 - * The worst-case scenario
 - * The most likely scenario
 - * A wildcard scenario
- 3** Divide your whiteboard or paper into quarters for each of these four scenarios. Then, capture key points about what each one might involve. This relies on some informed guesswork, but see if you can at least identify clear signals for each scenario. **The goal is to clarify for you or your team how they can assess a potential incident in the future, which will help everyone know the next steps to take.**

PLANNING FOR PEOPLE & PURPOSE

The focus of any forward planning is always to protect the *people* involved and stay anchored in the *purpose* of your event or action. When things feel overwhelming, zooming in on these two areas and breaking down what you will do *before, during and after* an event can help refine and clarify your plans.

Here's an example of an organisation that has been the subject of false information campaigns in the past. Their small communications team are planning to launch a research report and undertake media commentary about their findings.

EXAMPLE:

MOST LIKELY SCENARIO

"An overall successful report release, but encountering a spike of false information about our research and some harassment (but not direct threats) aimed at our spokespeople."

PLANNING FOR PEOPLE

BEFORE

- * Ensure all our spokespeople review their online presence and potential access points.
- * Undertake internal communications to ensure everyone feels informed and included in our safety planning.
- * Prepare wellbeing plans for spokespeople and team members who are responsible for monitoring our public engagement.

DURING

- * Ensure our spokespeople's inboxes and accounts are monitored by other team members.
- * Assess and report any harassment. Direct threats indicate we move to a worst-case scenario plan.
- * Ensure people who are responsible for monitoring have a roster and clear contacts for extra support.

AFTER

- * Ensure our monitors and spokespeople have the option for a debrief session to capture what people's experiences were.
- * Enact any wellbeing plans as needed.

PLANNING FOR PURPOSE

BEFORE

- * Share our purpose of the report launch and measures of success internally with everyone involved.
- * Develop proactive and reactive messaging about any false information we anticipate.

DURING

- * Ensure accurate information and reactive messaging is available to all our stakeholders, the general public and the media.
- * Stay anchored in our purpose and measures of success.

AFTER

- * Circle back to purpose and our measures of success.
- * Share internally anything we learned that may help in future report releases.
- * Share externally any successes which help promote the purpose of the event - for example, great media coverage of our report.

ESCALATING THINGS

Escalation planning is all about deciding when to ask for help or take your most serious actions in response to an incident. The most important part is to agree on what these actions are, how to assess them and who you can contact for support.

It's important to be realistic about what you or your organisation can be responsible for responding to. For example, a 'worst-case' scenario for most people involves receiving a death threat or holding an event where a violent incident occurs. However, very few organisations have the training and resources to deal with such serious risks.



Keep in mind that law enforcement and digital harm prevention agencies exist specifically to help you respond to things like this. You don't need to be a safety or security expert, but you do need to decide when you will reach out to one, and think ahead about who your specific support network will include.



Basic escalation plans should include:

Definitions:

Decide what constitutes harassment or false information campaigns for your purposes. For example, experiencing persistent unwanted messages and threats or being subject to organised efforts to spread false information.

Record keeping & evidence:

Decide how you will record and store evidence of harassment. For example, your assigned monitors might record evidence in a central folder containing emails, screenshots, timestamps and URLs.



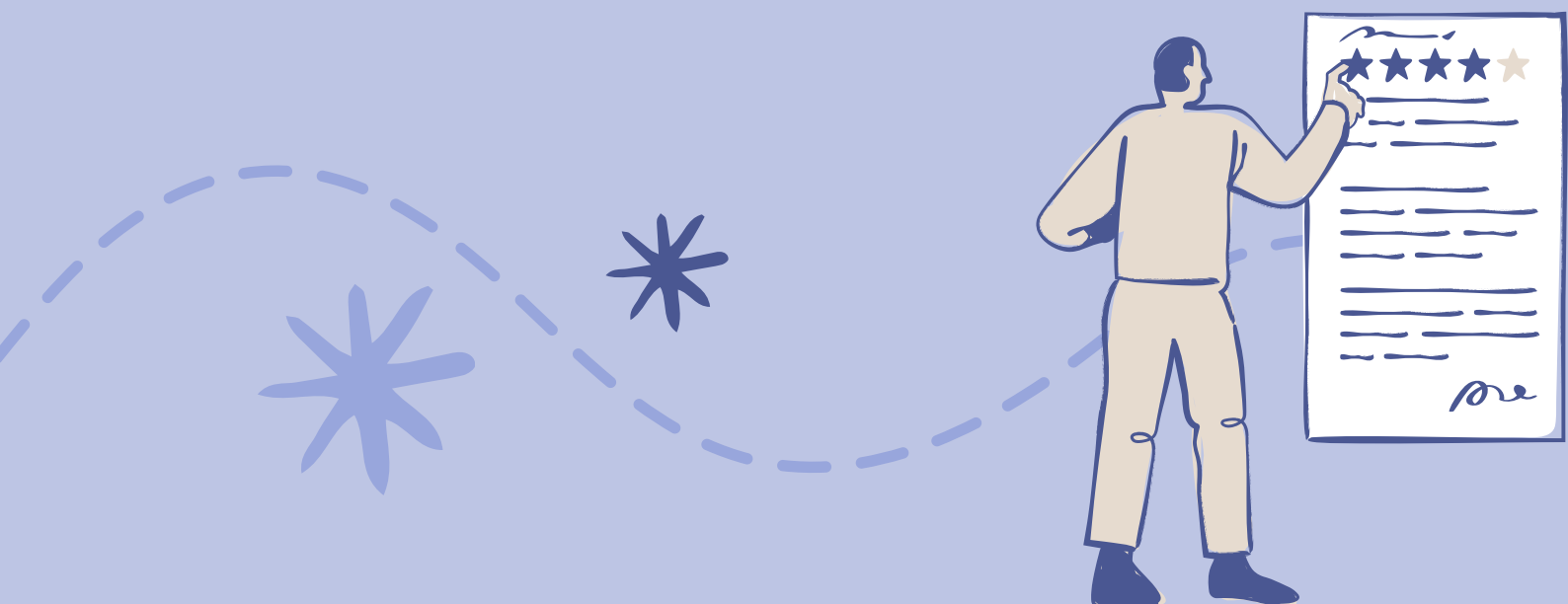
Another way to record evidence is to use your phone camera to record any in-person harassment. However, it's important to use good judgment about when it's safe to do this. For example, if only one person pulls out their phone to record, they may become a target themselves. Consider whether one person recording becomes a signal for other organisers to record.

Roles & contacts:

Clarify internally the people and roles responsible for making decisions and enacting plans for your organisation. Externally, identify contacts like security guards or Police liaisons. Include links to any external reporting forms you might need to use.

RESOURCES

- * [Community safety plan template | Amnesty](#)
- * [Escalation Process Template | Screendesk Blog](#)
- * [Threat and Risk Guidance | Protective Security](#)
- * [Practical threat modelling exercises | UoT](#)





COMMUNICATIONS

Internal messaging

In high-pressure moments, confusion inside organisations can sometimes create more stress than the incident itself. Any action or event that involves a team of people should have:

- * Regular meetings leading up to your event or action, and clear staff communications about your plans and approaches.
- * An internal communications channel that can be stood up during incidents, for example, a group chat for updates and instructions. Make it clear who needs to be in this channel.
- * Agreement on who is authorised to speak publicly and post responses online, and who will sign off on messaging, or support them to do that.

Incidents often escalate because one well-meaning person steps outside agreed roles. With that in mind, basic internal communications ahead of any action or event should involve:

- * A pre-event briefing of all staff and volunteers.
- * Clarifying what not to do (e.g. staff don't debate detractors online).
- * Ensuring casual staff or volunteers understand escalation channels.

External messaging

It's important to plan ahead for what false information may be spread about you, your work or your organisation. There are a range of communications approaches to mitigate and respond to false and harmful information, so use the resources listed later in this section to consider what options best suit you.

Here are some key principles of good communications in the face of a challenging environment:

- * List all the opposing points you can think of, and prepare messaging that can help you address or respond to those arguments.
- * Stay clear about who your audience is and isn't.
- * Be realistic about refuting false information. It's not always appropriate or possible to change people's minds, and it's unlikely that you or your organisation are the appropriate people to combat the extreme beliefs of others.
- * Stay anchored in your purpose. Celebrate and showcase your strengths and expertise whenever possible.
- * **Remember that most people trust and value the expertise and experience of others. Frame your messaging with these people, rather than bad actors, in mind.**

RESOURCES

- * [Recommendations for Countering Misinformation | APA](#)
- * [Crisis Communication in the Age of Disinformation | WebStat](#)
- * [Tackling Mis/Disinformation | ICCO PR](#)
- * [Countering Disinformation Effectively | CEFIP](#)
- * [Disinformation in the City | UoM](#)
- * [How Mindset and Narrative Shifts Can Enable Change | The Workshop](#)

WHAT HAPPENS AFTERWARDS?

While most of your efforts are put into planning for, and responding to, online harm, what happens afterwards can be just as important. Ask yourself the following:

Debriefing & evaluations

- * Would your team benefit from a debriefing session?
- * How will you ensure this is a safe and constructive meeting?
- * How will you return to your measures of success when reflecting on your action or event?

Sharing

- * How will you capture and share what you learned?
- * Are there similar organisations who would benefit from hearing about your experience? Could this be an opportunity to upskill others?
- * How will you celebrate your successes and reward the effort your team put into planning for this event or action?

Continued impacts

- * How will you monitor any continuing risks that may have arisen? Consider setting a defined monitoring window after major events (e.g. two weeks). You may wish to create and maintain a simple risk register to keep track of any issues.
- * When will you stand down any heightened monitoring? What are your thresholds for re-escalation?
- * Are your wellbeing plans working as intended? (More info in the next chapter).
- * If false claims gained traction, do you need to rebuild public confidence and offer clarifications in calm moments rather than reactive ones?
- * Can you collaborate with supporters or partners to amplify corrective messaging?

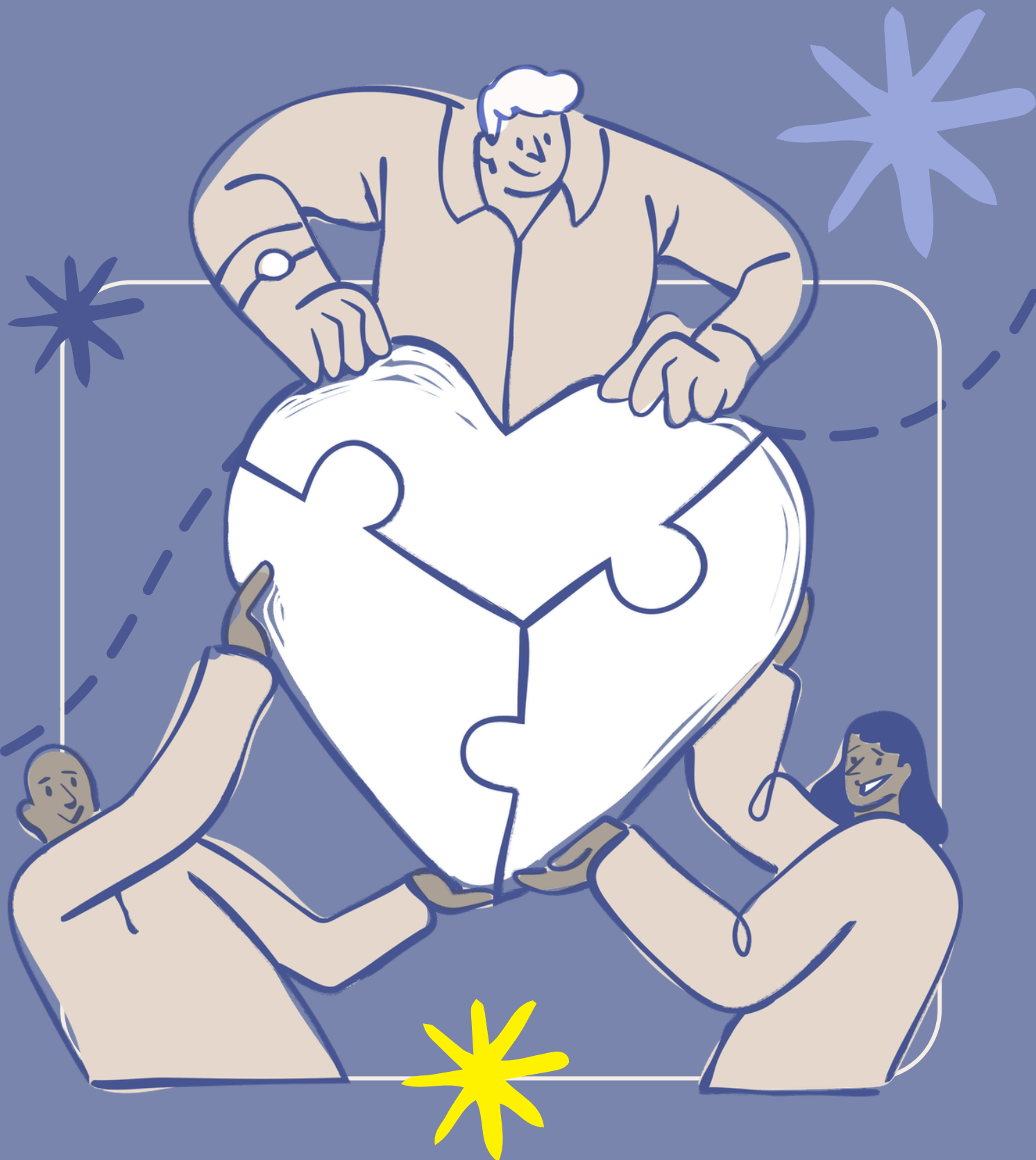


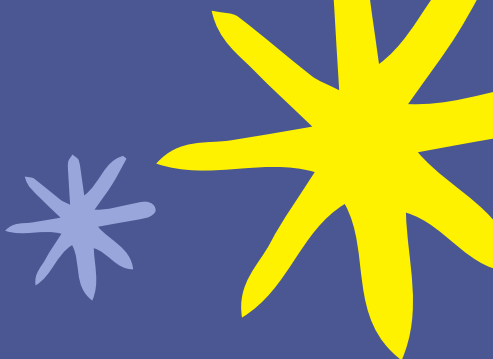
RESOURCES

- * [What is a Debrief Meeting? | Guidebook](#)
- * [Organisational Debriefing Guide | Civil Defence](#)
- * [Conducting Debriefs | NSW Public Health](#)
- * [Event Review Template | Amnesty International](#)

CHAPTER FOUR:

WELLBEING





KEY POINTS FROM THIS CHAPTER



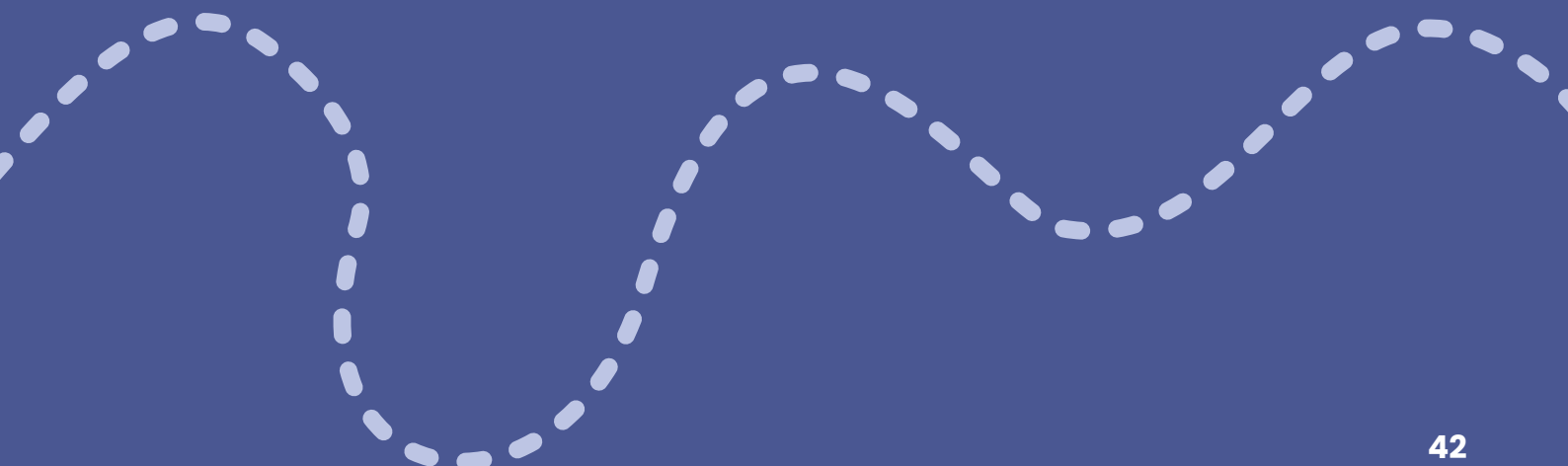
It can be upsetting and impactful to respond to harm and harassment, but planning ahead for your wellbeing is important.



Safety and wellbeing are interconnected ideas. You can't have a robust safety plan without considering how your people will stay well in the face of harm and harassment.



Creating a wellbeing plan is simple. The hard part is being encouraged to use it, so it's important to normalise wellbeing as part of safety planning.





THIS SUCKS

Let's be honest, not only is it scary and tiring to have to respond to harm and harassment, but it's also understandable to feel a sense of grief or disbelief at the level of polarisation and hatred present in some parts of our society. This sucks.

In the long-term, your organisation should consider how to adapt your priorities, allocate your resources, and shift staff culture to stay resilient in the face of this new normal. However, in the shorter term, your focus should be on supporting the targets of false information and harassment, and the people responsible for monitoring and responding to that on behalf of your organisation.

Safety is wellbeing

Experiencing threats and harassment can significantly affect people's emotional and physical health. Repeated exposure to harmful content can have lasting impacts. **This means wellbeing isn't optional. It's a core part of safety planning.**



NO SURPRISES

Successful safety and wellbeing planning helps to remove the element of surprise. While it's normal to feel shocked and frightened in the face of harm and harassment, having a safety plan can soften that shock and reduce any confusion about how you should respond. This clarity is hugely valuable in times of stress.

The ultimate goal of any plan is to account for what you and your organisation needs to feel informed, empowered and supported to do your best work, even if the environment is challenging.



HOPE FOR A GOOD TIME, PLAN FOR A BAD TIME



A great place to start with your wellbeing plan is to think about how you might feel at the end of a difficult day — or week — of targeted harassment. What support would you need?

A basic wellbeing plan might answer:

- * What situations could lead to you needing to enact your wellbeing plan?
- * What are the early signs you may be starting to experience stress/poor mental health?
- * What things have contributed to your wellbeing (positively or negatively) in the past? Remember that this extends beyond your basic physical needs, so consider your emotional, spiritual, social and workplace wellbeing.
- * What are the activities, mindsets and resources which you can draw on to support your wellbeing?
- * Who are the people you can reach out to if you need support? How will you share this plan with them ahead of time?

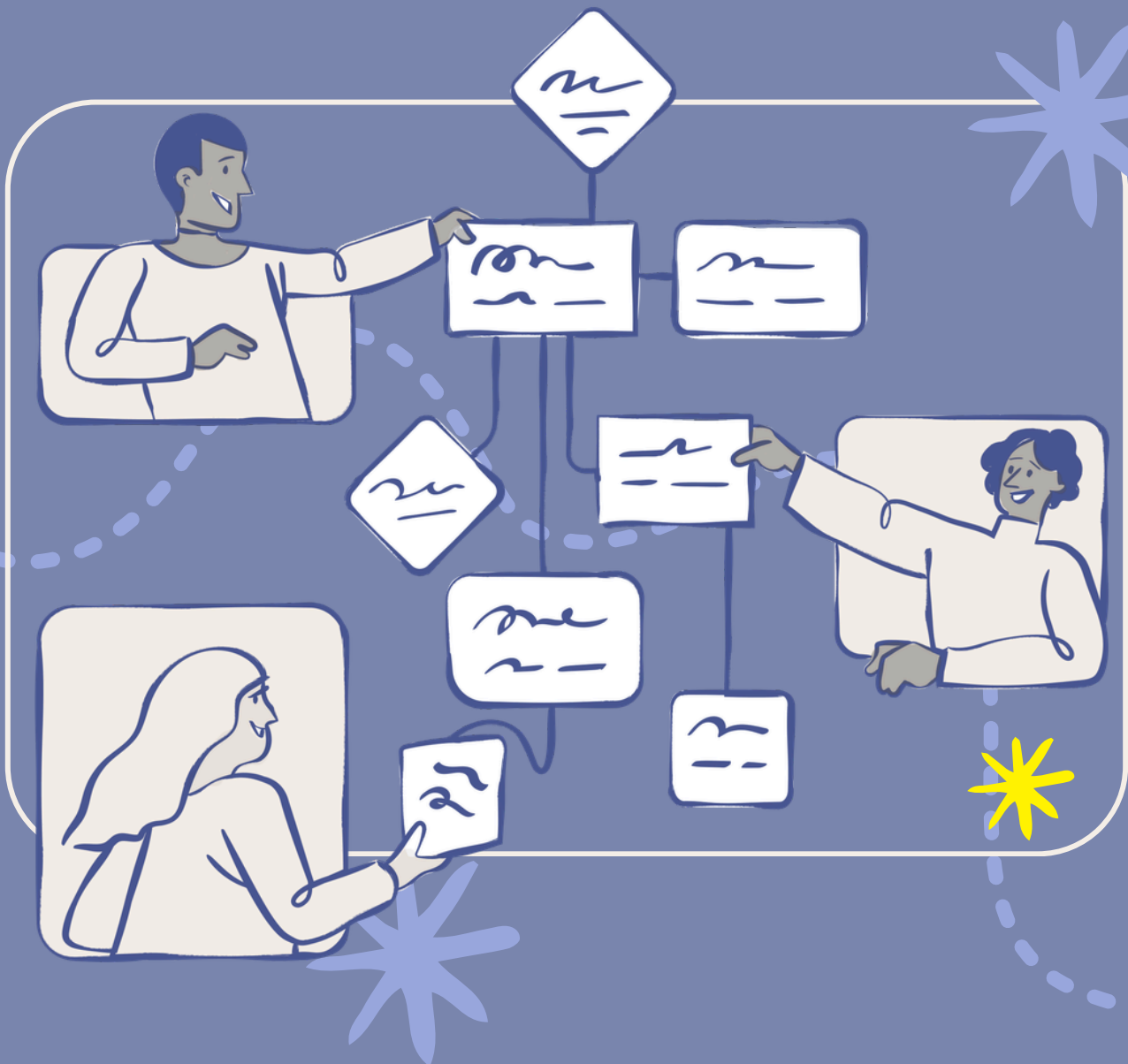


RESOURCES

- * [Te Whare Tapa Whā | Ministry of Health](#)
- * [Resources to Support Wellbeing Planning | MHF](#)
- * [Online Abuse in the Workplace | Safe Work Australia](#)
- * [Mental Health Care Kit | Stop Online Harm](#)
- * [Mental Health Action Plan | Mental Health UK](#)
- * [Advice from a Psychologist | PEN America](#)
- * [Online Community Moderators Managing Harm | Netsafe Resources | Global Center for Journalism & Trauma](#)

CHAPTER FIVE: IN THE MOMENT

A STEP-BY-STEP GUIDE TO DEALING WITH HARASSMENT





DEALING WITH HARASSMENT

STEP ONE: Assessment & documentation

- ➔ Make a safety assessment. If there is a direct threat of physical harm or someone is threatening to come to your location, call 111 immediately.
- ➔ Document everything. Take screenshots of abusive messages, comments, and profiles, including timestamps and URLs wherever possible.
- ➔ Hide, but don't delete, the abusive content. It can be useful to have evidence of harassment.
- ➔ Determine if it is a single incident or a sustained campaign. Note if the harassment includes threats of violence, doxxing or sexual harassment.

STEP TWO: Mitigations

- ➔ Immediately mute and block the accounts involved on all platforms.
 - ➔ Assess whether you need to change your privacy settings to restrict who can comment on or see your posts.
 - ➔ Don't engage with the harasser, as this can fuel further harassment.
 - ➔ If the harassment is happening on social media, report it using the platform's reporting function. Select the most accurate reporting option (e.g., "harassment" or "targeted abuse") and document the reference numbers for your reports to the platforms.
- 
- 



DEALING WITH HARASSMENT

STEP THREE: Escalations

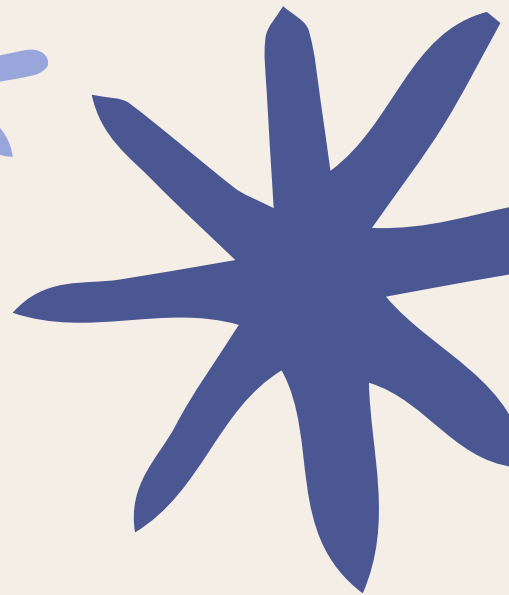
- ➔ If you've made an escalation plan, now's the time to enact it.
- ➔ Regardless of whether you file a police report, consider reaching out to organisations that can help with online harm.
- ➔ Depending on the severity of the harassment, consider speaking to a lawyer about options for legal action.

STEP FOUR: Wellbeing

- ➔ If you've made a wellbeing plan, now's the time to enact it.
 - ➔ Tell trusted friends, family, or colleagues what's happening and how you're feeling.
 - ➔ Try and keep perspective. Remember that people who talk a big game online are deliberately trying to scare you. Try to stay clear on your purpose and your measures of success.
 - ➔ Take breaks from social media and consider asking for help monitoring your channels.
- 

RESOURCES

- * [Download step-by-step guide as a poster](#)
- * [How to Record Digital Evidence | Netsafe](#)
- * [Harmful Digital Communications | Ministry of Justice](#)
- * [Cyberbullying Protections | Community Law](#)
- * [Procedure to Respond | Researcher Support](#)





Tāhono Trust (formerly Inclusive Aotearoa Collective) is an organisation working to connect and empower communities across Aotearoa me Te Waipounamu.

Our work is centred on Te Tiriti o Waitangi, and we support and deliver social cohesion efforts across the country. We do this through facilitation, education, connection, administration, partnerships, and our Belonging Conversations research project.



Online harm affects both individuals and society. Without proper safeguards, digital platforms have created toxic environments that cause harm both online and offline.

#Noharmware is a joint campaign between Tāhono and Amnesty calling on the Government to regulate online platforms and hold tech companies accountable for harmful digital environments.

**AMNESTY
INTERNATIONAL**



Amnesty International Aotearoa New Zealand is part of a 10 million-strong global movement of people who stand for universal access to fairness, justice, dignity and inclusion – our essential civil rights.

Standing together, our shared humanity holds the power to create change.


Anchordown

Anchordown is a consultancy that helps organisations and communities prevent and respond to the growth of disinformation, online harm and polarisation.

We specialise in countering online harm by providing best-practice training and guidance that help organisations build great strategies and systems.

A dashed, light blue curved line that starts on the left side of the page and curves downwards and to the right, passing behind the text blocks.

This Safety Planning Toolkit is
© 2026 Tāhono Trust and
Anchordown. It is made available
under a Creative Commons
Attribution 4.0 International License.

This toolkit is designed for civil
society organisations, community
groups, academics, researchers,
and individuals facing online
harassment. You may download,
print and share this resource freely.

**When using or adapting content
from this toolkit, please attribute it
as: "Safety Planning Toolkit by
Tāhono Trust and Anchordown".
Please note that some external
resources referenced may have
their own terms of use.**