// GUIDE

HOW TO STAY SAFE

Local Government New Zealand's guide to protecting candidates and elected members from abuse and harassment

May 2025

Ko Tātou LGNZ.

INTRODUCTION >

Being an elected representative is incredibly rewarding and fulfilling but comes with some challenges. That includes being aware of potentially unsafe situations – both online and in person – and how to keep yourself safe.

It's also important to know that you don't have to deal with this alone. Elected members can access a range of support from LGNZ.

// THIS GUIDE HAS BEEN DESIGNED TO HELP YOU:

+ Protect yourself as a candidate ahead of local elections
+ Keep safe online and combat any abuse or harassment
+ Limit public accessibility to your personal information
+ Build a safety plan for public meetings and events
+ Develop strategies for dealing with situations when you're out on personal time
+ Know how to make a complaint, and to who
+ Access support networks and counselling.

Please note that the information contained in this guide represents advice, guidance and best practice as provided by LGNZ and agencies including the NZ Police, Netsafe and Elections NZ. It is not intended to replace any legal advice you receive regarding an active investigation or situation of abuse or harassment.

KEEPING SAFE ONLINE >

As a candidate or elected member, using websites and social media can be a great way to engage with your community. But it comes with risk and requires careful navigation, remembering that your use of these online tools is guided by the Code of Conduct and relevant laws.

In this section, we encourage you to think about:

- How to protect and limit your online personal data
- How to report a privacy breach
- Ways to mitigate harmful social media interaction.

Protecting your privacy

Consider risks from exposing private information

Your private information can potentially be exposed via social media accounts, websites, cars with election livery, election advertising and business cards. This can lead to:

- Phishing attempts (including via text message) to harvest your log-in details or banking details
- Unauthorised access to online platforms or internal systems
- Online scams delivered by messaging platforms such as Facebook, Instagram, or Whatsapp
- Disclosure of your, or your family's, personal information (including physical addresses)
- Whānau and friends' details being found and revealed.

Remember that information can remain online indefinitely. After an election, neglected accounts can lead to the same risks happening over the long term.

Mitigation: Personal vs public profiles

Public-facing profiles and collateral, both online and offline, are a rich source of data that can be collected for both legitimate and illegitimate purposes. As a public figure, we recommend you:

- Separate your personal accounts from your public ones. A good example is creating a standalone Facebook page specifically for your candidate campaign or elected member persona
- Create a completely separate email account for your public campaign or platform
- Consider using a new phone number or PO Box, especially if these are linked to a public profile
- Turn on privacy functions on all your personal accounts to limit who can interact with you online; this includes locking your Facebook and Instagram profiles
- Ensure your accounts are protected with strong passwords and two-factor authentication
- Ensure that up-to-date antivirus software is installed on any device used to access your email
- Don't open attachments or click on links in emails or social media messages from strangers or if you're unsure that the sender is genuine.

Action: If your personal information has been breached

There are several steps you can take if you believe your personal information has been compromised:

- If you believe you have been a victim of a phishing or text scam, you can report an incident to Cert NZ; fill out an online form here
- If you discover someone is impersonating you online, contact the platform (eg Meta or Twitter/X) as soon as possible
- If you believe your privacy has been breached, you should contact the Privacy Commission; phone 0800 803 909 or email enquiries@privacy.org.nz
- You can also make a privacy complaint online here
- If you wish to have personal information removed from Google, you can submit a request here.

Using social media and messaging apps

As an elected member, it is important that you manage your social media presence in line with your role as a community leader. Your online presence reflects not just on you, but on your council and the people you serve.

Minimising harmful social media interaction

- Think before you post. Once online, content is permanent and can be reshared or misinterpreted. Even if you delete a post, someone might already have taken a screenshot. Avoid posting or messaging anything you wouldn't say in a public meeting
- Stay professional. You are responsible for your posts and interactions. Follow council policies, respect confidentiality, and do not use council logos or official symbols on personal accounts
- Engage responsibly. Direct service inquiries to official council channels, avoid online arguments, and maintain respectful interactions with the public
- Don't retaliate. Most bullies are looking for a reaction, so don't give them one
- Don't keep harmful interactions a secret. Talk to someone you trust, such as a close friend, family member or counsellor, who can give you the help and support you need
- Document and save. If someone has posted something problematic, you can print or take a screenshot of it in case you need to share it later
- Prioritise privacy. Protect your personal information, respect the privacy of others, use strong security settings, and report any threats or harassment through the appropriate channels.

Understanding the Harmful Digital Communications Act

The Harmful Digital Communications Act sets out 10 principles that apply to texts, emails and online posts – what the Act calls 'digital communications'. NetSafe, as the cyberbullying complaints agency, takes these principles into account when considering a complaint. If complaining to NetSafe doesn't solve the problem and you decide to take your complaint to the District Court, the judge will take these principles into account.

The principles say that digital communications that are either sent to you, or are about you, shouldn't do any of the following things:

- give out sensitive personal information about you
- be threatening, intimidating or menacing
- be grossly offensive, as judged by any reasonable person in your position
- be indecent or obscene
- be used to harass you
- make false claims about you
- contain information or material that you had given to someone in confidence
- encourage other people to send you a message for the purpose of causing you harm
- encourage you to kill yourself
- put you down ("denigrate" you) on the basis of your colour, race, ethnic or national origins, religion, gender, sexual orientation or disability.

In addition, the Harassment Act covers harassment and intimidation across a wide range of different forms, whether it's through texts, emails or online posts, or through face-to-face harassment, stalking or letters. The Act says it applies where someone leaves offensive pictures or text where you'll see it, and this specifically includes online material.

The protections in the Harassment Act have sometimes been used in cases of online harassment. The Act allows you to apply to the District Court for a Restraining Order to stop the harassing behaviour.

Action: Reporting online abuse and harassment

If you have received abuse or harassment online that you feel constitutes a threat to your safety or to your family and friends, then you can choose to escalate this in several ways:

- If you believe content posted about yourself on either Facebook or Instagram has breached Meta's Community Standards, you can report the issue to the platform
- If you wish to make a complaint with regards to content posted on Twitter/X, you can do so here
- You can report bullying and harassment to Netsafe using this online form or by emailing help@netsafe.org.nz or texting 'Netsafe' to 4282. Netsafe can also provide you with advice if you've received abuse from fake social accounts
- You can choose to block any phone numbers, email addresses and social media accounts that are being used to send you harmful messages, as well as disabling comments on posts and videos
- If you've suffered serious emotional distress because of online material, you can apply to the District Court for it to take action to fix the problem – for example, by ordering the material to be taken down or ordering the person responsible to apologise to you. To be able to go to the District Court you have to have first complained to NetSafe and given them a reasonable chance to assess your complaint and decide what to do.
- More information about applying to the District Court can be found here.

Find more resources

- Akona Module: Stepping into Local Leadership Part 2: The life of an Elected Member
- Akona Zoom recording: Keeping yourself safe: online harassment and safety
- The Ministry for Women has recently released an Online Harm toolkit for Women.

KEEPING SAFE IN PUBLIC SETTINGS >

Whether you're a candidate or an elected member, it's important that you take steps to keep yourself safe when in public.

This is especially important if you're campaigning or taking a strong position on a divisive or controversial issue, or if you're attending a public meeting where a controversial topic is on the agenda.

You may even be at the supermarket or at your child's sporting event; it's possible in any of these settings that you'll encounter residents who are upset or angry, which may lead to unwanted confrontations and potentially threatening behaviour.

To prepare yourself for the possibility of this happening, we encourage you to:

- create safety and security plans to keep yourself safe
- learn about how you can mitigate unwanted behaviour
- learn about your options if you believe the situation is a genuine threat to your safety.

Staying safe in public and at home

As an elected member, you are a public figure. Your role is to engage with your community, but it's equally important to ensure your personal safety.

Having a plan in place can help you manage risks and feel confident in your role; it can also allow you to set boundaries and stay in control.

Staying safe at public meetings and events

Scenario: You're attending a public meeting where a controversial topic, such as a new rates proposal, is on the agenda. Residents are upset, and tensions in the room are rising.

Best practice is to:

- Have a support plan. If you're attending a public meeting or event where strong opposition is expected, coordinate with council staff, security, or fellow elected members ahead of time
- Be aware of tone and body language. Stay calm, neutral, and measured in your responses. Even non-verbal cues (e.g. crossed arms, eye rolling) can escalate tensions
- While engaging with the public is part of the role, you don't have to respond to every comment or question straight away. Stay professional, de-escalate tense situations, and know when to step away or seek support
- Don't engage in personal confrontation. If an individual becomes aggressive, de-escalate by acknowledging their concern and redirecting to appropriate channels (e.g. "I understand this is an important issue for you, have you submitted feedback through the official consultation process?")
- Know the venue layout. Identify your exits, what security presence there is (if any), and areas where you can safety step away to if needed
- Capture all this information in an event plan, so that all council staff, venue operators and security are aware of the risks and how to react if a situation occurs.

Dealing with situations when you're out on personal time

Scenario: You're approached in a public place, such as a supermarket or sports event, by a resident who is upset about a council decision. They start raising their voice, and bystanders take notice.

Best practice is to:

- Stay calm and polite. Lowering your voice can help diffuse tension. If they escalate, suggest continuing the conversation at another time or in an appropriate forum
- Be aware of tone and body language. Stay calm, neutral, and measured in your responses
- Set clear boundaries. "I'm happy to discuss this during office hours. You're welcome to contact me via email so we can set up a time."
- Leave the situation if necessary. If someone becomes aggressive or refuses to respect boundaries, remove yourself from the situation. If you feel unsafe, seek assistance from bystanders or security. Don't place yourself into any situation where you are alone with an aggrieved person without bystanders present
- Report any incidents. If harassment or threats occur, notify council staff and, if necessary, the police.

Avoiding unwanted attention at home

Your home or residence should be a safe place for you and your family. In the unlikely event that your home is placed at risk due to you being a candidate or elected member, there are measures you can take to protect yourself from harm.

Best practice is to:

- Limit your personal details available online or through other channels accessible to the public. This includes any candidate promotional materials, business cards, social media and information stored on the electoral roll
- Consider where you park cars with campaign branding
- Secure your doors, windows, sheds and garages with good quality locks. Install security stays on windows, especially those on ground level. The NZ Police offers a handy Home Safety Checklist
- Consider installing security cameras, motion detection lighting, home alarms and remote door cameras (eg. the Ring camera)
- Practice good security at your home or residence. Don't answer the door for someone you don't know or don't want in your home. Ask for identification if they say they represent a company. If you're outside for an extended time, eg. in the garden, lock your front door
- Don't open up any unexpected or suspicious packages delivered to your home or residence; if you believe they represent a genuine risk to your safety then contact the Police on 111
- Consider developing a home safety plan for you and your family. This should detail how you and family use security to ensure a safe home environment, and how to respond to any unwanted situations if they occur
- Report any incidents. If any harassment or threats occur in your home or residence, or if you believe that someone has unlawfully accessed your property, then immediately notify the police on 111. This includes any threatening phone calls or letters you receive.

Definition of harassment and applying for a restraining order

If you're being harassed by someone you're not in a relationship with, you can apply for a restraining order. Harassment has a legal definition as per the Harassment Act 1997. On at least two separate occasions within a period of 12 months, the harasser needs to have committed "specific acts", like:

- following you
- entering your property without your permission
- unwanted or threatening phone calls or letters
- giving you offensive material
- doing something that makes you fear for your safety.

Harassment is limited to intimidating behaviour — if the person has attacked you or destroyed your property, talk to the Police about criminal charges.

If you are the victim of harassment as defined above, there are a few options available to you:

- Apply for a restraining order. You can apply to the District Court for a restraining order if you're being stalked or harassed by someone and fear for your safety. A restraining order legally prevents that person from contacting you, and can also be used to protect your children if you're worried about their safety
- Restraining orders apply to a single harasser – if more than one person is harassing a victim then the victim will need to obtain harassment orders for each of the harassers. A restraining order only applies to harassers who are 17 years or older and is typically active for a period of one year, unless a court orders a different time period
- To apply for a restraining order, you need to complete these forms from the Ministry of Justice, which includes an application for a restraining order, notice of proceeding and an affidavit. You will need to sign the forms, or have your lawyer sign the forms, in front of a Justice of the Peace or Deputy Registrar, and then take the document to your local District Court
- If you do not know the name or address of the person harassing you, you can make a complaint to the Police with any information you have that could help them find and identify the harasser, including what they look like or where you've seen them
- If the Police have reasonable grounds to believe they've identified the harasser, they can make them give their name and address. If the person refuses or gives false information, they can be fined up to $500, and arrested if they continue to refuse after the Police have warned them
- You can keep your address confidential by filling out a form you can get from your local District Court — this means the court will know your address, but the person the order is against will not get a copy. Once you have a restraining order, you can choose not to have your name published on the electoral roll.

The unpublished roll

If you're concerned about your personal safety, or that of your family, you can apply to go on the confidential unpublished roll to ensure your address details are not available to the public.

Going on the unpublished roll means your details won't be included on printed electoral rolls. It also means you won't be able to check or update your enrolment details online. You'll need to make a special vote at parliamentary and local elections.

Find out how to apply to go on the unpublished roll here.

Sovereign citizens

Sovereign Citizens or SovCits are a group of people who believe that elected governments do not have legitimate authority and that they are exempt from New Zealand laws. SovCits often use pseudo-legal information rooted in historical laws and principles like the Magna Carta. They may deluge councils with paperwork in an attempt to evade legal obligations. Council staff and elected members are experiencing an escalation in extreme demands and threats from SovCits. This has included:

- Refusing to pay rates or fines, or falsely claiming land ownership under 'allodial title'
- Serving notices, affidavits, and what they call 'self-executing contracts' on councils
- Harassing councils with vexatious Official Information Act requests
- Writing threatening letters to elected members, sometimes to their home addresses
- Attempting to serve fictitious papers to council staff or elected members at their home, workplace or in public
- Attempting to access council premises using fake ID.

It's important to note that sovereign citizen theories and arguments have no legal basis in New Zealand and are rejected by courts. Anyone claiming to be a sovereign citizen or using pseudo-law to challenge a council charge or process will not remove any obligations to comply with the laws of New Zealand.

All of the advice contained in this guide can be applied to your interactions with SovCits. Additionally, your council should have a security plan in place for your premises. Key things to remember include:

- Be aware of your personal safety wherever you are; this includes your home, place of work or in public
- You are under no obligation to accept any notices, affidavits or 'self-executing contracts' from SovCits. These are not legal documents and the recipient is under no obligation to receive, read or abide by the contents of them
- Immediately report any threatening correspondence or confrontations with SovCits to the NZ Police.

Other resources

- Akona Zoom recording: Keeping yourself safe: physical safety and security
- Akona Zoom recording: Keeping yourself safe: "sovereign citizens" and vexatious requests

SUPPORT NETWORKS AND COUNSELLING >

As an elected member, you don't have to navigate this road alone; you have access to a range of support networks and other services throughout your tenure.

The following support is available to all LGNZ member councils.

LGNZ support networks and information

- **Te Maruata** connects Māori elected members and serves as LGNZ's Māori advisory group, advocating for increased Māori representation and participation in local government, while supporting councils in building authentic relationships with iwi and hapū
- **The Young Elected Members (YEM) Network** connects members under 40, offering networking and development opportunities, and advising on issues affecting young elected officials
- **The Community Boards Executive Committee (CBEC)** advocates for community boards nationwide, supporting their development and impact
- LGNZ manages a private Whatsapp group for Women in Local Government. If you'd like to be added to this group, please contact info@lgnz.co.nz
- Elected members can access LGNZ's **Akona** platform, which includes modules, zoom recordings and other learning materials to help keep candidates and elected members safe.

Other support networks and information

- **Netsafe NZ** offers a range of resources to help protect you from online harm, and can provide advice on making a complaint and increasing your online security
- **Elections NZ** offers security advice for candidates during their candidacy period
- **The NZ Government** offers advice on addressing abuse and harassment
- **The Human Rights Commission** can also provide support and advice if you have issues relating specifically to your rights
- The **NZ Police** website contains information about what to do if you're experiencing threats of physical harm or intimidation.

Counselling

Being an elected member puts you on the front line in your communities, which can take its toll on your health and wellbeing.

LGNZ offers a free counselling and support service for any elected member who needs it. You have free access to a 24/7 helpline and online resources, including digital tools to help track and manage your wellbeing, whether you're focused on reducing stress, managing anxiety, improving your sleep or supporting loved ones.

Your details remain fully confidential — no identifying information is shared with LGNZ or your council.

- Access wellbeing tools here. Use the code 'LGNZMember' and password 'wellbeing'
- Find a therapist. Please click here to access a TELUS health clinician.

Tell us about your experiences

LGNZ is here to help if you're experiencing issues with abuse or harassment. We can provide advice and direct you to support services.

If you wish to reach out to us for support, please contact the team in confidence at info@lgnz.co.nz.

LGNZ also runs member surveys to help understand the extent of this issue and support our advocacy for system change.

If you have other information or tips on how to stay safe, let us know for the next version of this guide.


Ko Tātou
LGNZ.