Safeguarding your community organisation against foreign interference

Toolkit for community organisations

Ministry for Ethnic Communities
Te Tari Mātāwaka

CONTENTS

About this toolkit

Purpose of this toolkit

Community organisations play a vital role in supporting communities and driving positive change. Because of their important work and connections, community organisations in New Zealand can be targeted by foreign states conducting foreign interference.

This toolkit is designed for everyone in your community organisation—from leaders and board members to staff and volunteers. It offers practical tips and checklists to help you recognise risks and safeguard your organisation.

Who can use this toolkit?

Everyone has a role to play in keeping New Zealand safe from foreign interference.

The toolkit is divided into two sections which include practical tools and checklists:

- **For leaders:** focusing on their key responsibilities in guiding and protecting the organisation
- **For all team members:** to be mindful of any risks that could be linked to foreign interference.

Being informed, not alarmed

Foreign interference can take many forms and isn't always easy to spot. **See:** Examples of foreign interference

Being aware and able to recognise potential foreign interference risks helps protect your organisation by identifying genuine threats.

The New Zealand Security Intelligence Service (NZSIS) has released their latest New Zealand Security Threat Environment assessment. It includes advice to increase resilience to the threat of foreign interference. **See:** New Zealand Security Threat Environment

What is foreign interference?

The New Zealand Security Intelligence Service (NZSIS) defines foreign interference as an act by a foreign state, often acting through a proxy, which is intended to influence, disrupt or subvert New Zealand's national interests by deceptive, corruptive or coercive means.

Normal diplomatic activity, lobbying and other genuine, overt efforts to gain influence are not considered foreign interference. Learn more: Foreign interference in New Zealand.

Keeping your community organisation safe from foreign interference

Why are community organisations at risk from foreign interference?

Community organisations often play a vital role in supporting and shaping communities, influencing decision-making, and connecting diverse groups. Their extensive networks and trusted relationships make them key players in community leadership and engagement.

Foreign states engaging in interference may target community organisations in New Zealand to deceptively, corruptively or coercively:

- Access personal or sensitive information about the organisation or community members.
- Undermine social cohesion and negatively impact communities in New Zealand.
- Suppress views that oppose those of a foreign state's interest.
- Gatekeep or control access by influential community leaders and individuals.
- Influence their leadership, strategic direction, communications and engagement.
- Infiltrate the community organisation to advance their own interests.
- Leverage the organisation's relationships with decision-makers and the wider community.
- Create internal divisions to weaken the organisation's effectiveness and reputation.
- Recruit influential individuals within the organisation to advance their own interests.
- Spread disinformation or misinformation through the organisation's networks.
- Interfere in general and local elections.

Resources for communities about foreign interference are available on the Ministry for Ethnic Communities website in 30 languages.

For your community organisation to consider:

- Why would a foreign state target my community organisation or my role **to deceptively, corruptively or coercively advance their own interests?**
- What **part of our structure or information could a foreign state target** to deceptively, corruptively or coercively advance their own interests?
- Is there anything about **my role, or my organisation's role, influence, or public voice that could be targeted** by a foreign state trying to deceptively, corruptively or coercively advance their own interests?
- **Could foreign states see our organisation as a gateway** to communities, decision-makers, community leaders, or public opinion?
- **Are there specific causes or issues** where our voice is particularly influential, which could attract unwanted attention from foreign states conducting foreign interference?
- How could a foreign state use **our work, connections, or access to information** to deceptively, corruptively or coercively push interests that conflict with our organisation's or New Zealand's values?

Keeping your community organisation safe from foreign interference

Safeguarding your community organisation

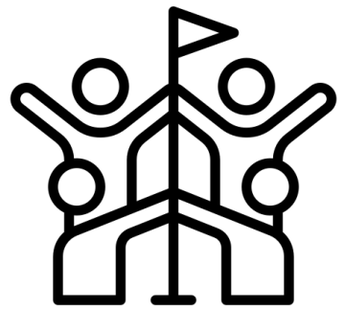
Community organisations often operate with limited resources and volunteer-led structures. Recognising the risks of foreign interference isn't about taking on national security responsibilities — it's about identifying any vulnerabilities and strengthening your organisation to protect your members and mission. Even in small, volunteer-led groups, simple practices such as discussing emerging risks, keeping records of decisions, and maintaining clear processes, roles, and responsibilities can make a difference in building resilience to foreign interference.

Maintaining good governance practices

Good governance practices are key to building a resilient community organisation.

Transparency, accountability, and informed decision-making not only support effective management but also help reduce the risk of foreign interference.

A strong board is one that works well together, stays connected to the community, and remains alert to emerging issues, such as foreign interference. By encouraging open dialogue and actively monitoring risks, boards are able to play a critical role in protecting their organisation.



Staying vigilant is everyone's role

Protecting a community organisation from foreign interference isn't the job of one person or role — it's a shared responsibility.

Whether you're on the board, part of staff, or a volunteer, staying alert to the risk of foreign interference is part of maintaining a strong, trusted organisation.

Regular communication, asking questions, and sharing concerns help community organisations respond quickly and effectively to potential risks.

This collective awareness strengthens the organisation's ability to protect its mission and the communities it serves.

Key actions for guiding your organisation

Checklist for leaders

As leaders, you play a key role in guiding your organisation to withstand foreign interference. Here are some key actions you can take:

- **Know your organisation's value**. Consider what aspects of your community organisation might attract interest from foreign state actors — such as your influence, connections with communities and decision-makers, and access to important or sensitive information.
- **Assess your organisation's risk of foreign interference by identifying which people, information, or activities might be targeted.** Use a risk register to help guide this process.
- **Make sure all board members, staff, and volunteers understand what foreign interference is**, how to recognise its potential risks, and how it could affect your community organisation. **See** Information about foreign interference
- **Have clear and comprehensive policies** that set out how your organisation operates and makes decisions. This promotes transparency and consistency in how your organisation operates. **See** Policy Health Check
- **Have a clear and comprehensive** Code of Conduct to guide governance, employees and volunteers to maintain integrity and adhere to your internal policies. **See** Policy Health Check
- Encourage a culture **where vigilance and questioning unusual behaviour are part of everyday practice**. If something feels off, trust your instincts and tell someone.
- **Check decisions, partnerships, and funding opportunities against your organisation's values, strategy and priorities** to help your organisation maintain a clear direction in its decisions, activities, and partnerships.
- Have clear **policies for managing stakeholder relationships, donations and funding**. Make sure all board members and staff are aware of them and document any new relationships or contributions.
- **Scrutinise all donations, grants, funding and offers of support** to minimise the risk of inappropriate obligations, influence, expectations, or pressure being attached to them. **See** Checklist: Gifts, funding and donations
- **Ensure IT and cyber security systems and policies are up to date,** to help keep your systems and information protected from potential threats. **See** Key practices for strengthening IT and device security

Organisations are required to comply with relevant New Zealand legislation, such as the Charities Act 2005 and the Incorporated Societies Act 2022.
This information is intended to provide general guidance and promote understanding.

Building a speaking-up culture
Checklist for leaders

Staying vigilant is everyone’s role.

As leaders, make sure everyone in your community organisation knows they should **speak up early, ask questions and support transparency.**

Speak up early

- ❑ If something doesn’t seem right — even if you're unsure.
- ❑ About unusual or overly generous offers of funding, gifts, or donations.
- ❑ About requests or pressure to bypass normal decision-making processes.
- ❑ About inappropriate requests for access to sensitive information.
- ❑ If you feel pressured or uncomfortable.
- ❑ Know who to go to if you need to discuss a concern.
- ❑ Acknowledge and value those who speak up as this can encourage others to do the same.

Ask questions

- ❑ If an opportunity or offer feels too good to be true — trust your instincts.
- ❑ Check if new proposals, partnerships, or offers align with your organisation’s mission, values, and goals.
- ❑ Verify the background and reputation of new partners, donors, or external contacts.
- ❑ Consider how an offer or partnership might affect your organisation’s independence or reputation.
- ❑ Encourage open discussion among your team when something feels uncertain or unusual.
- ❑ Keep front of mind: are we staying true to our organisation’s mission?

Support transparency

- ❑ Make sure decisions are made in a transparent, accountable way.
- ❑ Keep records of key decisions, including who was involved and why they were made.
- ❑ Disclose potential conflicts of interest, even if they seem minor.
- ❑ Be clear about how and why the organisation engages with partners, funders, or stakeholders.
- ❑ Encourage open conversations about ethical concerns or grey areas.
- ❑ Stick to agreed decision-making processes.
- ❑ Create a culture where questions about decisions or processes are welcomed.

Policy Health Check

Checklist to identify gaps in your organisation's policies

Having well-defined policies can help safeguard your organisation from foreign interference by promoting consistency, accountability, and effective decision-making.

Regularly reviewing your policies to ensure they are working effectively and strengthening them as needed helps maintain strong standards and helps protect your organisation.

Check your policies

Key areas where established policies are essential:

- ❑ **Roles and responsibilities:** Define roles, responsibilities, process for governance changes and decision-making authority.
- ❑ **Conflict of interest:** Require disclosure and management of any external interests that could affect impartiality.
- ❑ **Membership criteria:** Set standards for vetting, like background and criminal record checks.
- ❑ **Transparency requirements:** Have clear processes to ensure decisions and funding sources are openly discussed and recorded.
- ❑ **Communication protocols**: Establish who can speak or negotiate on behalf of the organisation.
- ❑ **Amendment procedures:** Have clear processes to review and update the constitution and/or charter as the organisation evolves.
- ❑ **Reporting mechanisms:** Include formal channels for raising concerns about foreign interference or other concerning activity within your organisation.
- ❑ **Security provisions:** Clearly set out how your community organisation will protect and manage any sensitive information and assets.

Check your code of conduct

Key areas your code of conduct should cover:

- ❑ **Conflict of interest disclosures:** Require members to declare any relationships or interests that could affect their objectivity.
- ❑ **Gifts and favours policy:** Define the processes for handling gifts, favours, or donations, including clear limits.
- ❑ **Confidentiality rules:** Define how sensitive information should be handled and limit access to authorised individuals only.
- ❑ **Transparency and honesty:** Promote open communication and reporting of suspicious or unusual behaviour.
- ❑ **Raising concerns:** Ensure there are safe and confidential ways for individuals to raise concerns.
- ❑ **Respect for organisational independence**: Emphasise commitment to the organisation's values and mission.
- ❑ **Professional conduct standards**: Clearly outline expected behaviours that reflect integrity and accountability.
- ❑ **Consequences for violations:** Clearly outline disciplinary measures for breaches of the code.

This content is adapted from information from Community Governance Aotearoa.
This information is intended to provide general guidance and promote understanding.

Key practices for staying vigilant

Checklist for everyone in your organisation

Everyone has a role to play in safeguarding your organisation from foreign interference

Awareness and vigilance

Is an individual being persistent or unusually interested in your organisation? Check out the New Zealand Security Intelligence's (NZSIS) S.O.U.P framework. Are they being **S**uspicious, **O**ngoing, **U**nusual and **P**ersistent? This may seem harmless at first but their approach could be well planned and take place over time.

Be cautious of individuals who ask detailed or persistent questions about your organisation's internal operations, staff, or community members without a clear reason. This kind of targeted questioning may be an attempt to gather sensitive information.

Ask yourself whether you're being asked to unduly influence others to support views that may not align with your organisation's values or interests. These kinds of requests can be subtle, so it's important to stay aware and reflect on their intent.

Report any concerning or suspicious behaviour to your leadership or board. If something doesn't feel right, trust your instincts and talk to someone about it. **See:** How to report foreign interference.

Due diligence

Do due diligence on individuals and organisations who approach you for a relationship, including other non-governmental organisations. **See:** Due diligence

Always consider the **background and motivation** behind any proposed support, funding, or investment. Foreign interference efforts may use **offers of assistance** to gain leverage or control over community organisations. **See:** Key practices for managing gifts, funding and donations

Pay attention to anyone who tries to bypass normal communication or decision-making processes — such as pushing for private meetings, avoiding written records, or discouraging others from being involved. These behaviours may signal an attempt to avoid transparency.

Before sharing information, take a moment to check where it came from. Verifying the source helps prevent the accidental spread of false or misleading content.

Continued on the next page

Key practices for staying vigilant

Checklist for everyone in your organisation

Everyone has a role to play in safeguarding your organisation from foreign interference.

Engage safely

Take a trusted colleague with you when meeting new contacts (online or in person) and keep them included in email exchanges.

Share only the contact details you're comfortable making public in your role. Keeping your personal contact details private can help protect your privacy, and reduce the risk of unwanted contact.

Do not discuss sensitive or private information in public or in places where others might overhear. This helps prevent the risk of that information being misused.

Step away from any conversation if you feel uncertain or uncomfortable. In an emergency, call 111.

Gifts, donations and favours

Be cautious with offers of gifts, funding, donations or favours — especially if they come with unexpected pressure or expectations. Some offers may be used by foreign state actors to gain influence, access, or leverage over your organisation. **See:** Key practices for managing gifts, funding and donations

Be consistent in how you handle offers and define this process. Clearly communicate your organisation's policies when gifts or support are offered, and apply the same process to all offers — regardless of who they come from.

Stick to your organisation's values. Decline offers that don't align with your mission or that come with strings attached — especially if those conditions involve obligations your organisation wouldn't normally accept.

Discuss offers as a group. If you're unsure about accepting an offer, raise it with your board or team before responding. Making decisions collectively can help reduce the risk of individual pressure or influence.

Continued from the previous page

Key practices for managing gifts, funding and donations

Checklist for everyone in your organisation

Anyone in the organisation can be approached with a **gift, funding, donation or favour.**
If you are offered something, consider:

Is there pressure to act quickly? If someone insists you accept an offer right away or discourages you from discussing it with others, that's a red flag. Legitimate support doesn't require secrecy or urgency.

Is there a lack of transparency about where the support is coming from? If the person or organisation offering can't (or won't) explain the source of the offer or seems vague about who they are representing, that's a sign to be cautious.

Do you feel uncomfortable or unsure? If something about the offer feels off, trust your instincts and raise it with your team.

Does the offer include requests for sensitive or detailed information about your organisation, community, or operations? Legitimate support typically doesn't require sharing private or internal details beyond what's necessary.

Are you discouraged from documenting or reporting the offer? If someone asks you to keep the offer informal, off the record, or "between us," take a moment to pause and consider why.

Does the supporter ask for involvement in your organisation's internal meetings or strategic planning in exchange for their offer? Be cautious if they expect roles or influence beyond what is appropriate for a donor or partner.

Does the offer seem unusually generous or out of proportion? If the support being offered is far more than the organisation typically receives or seems beyond what you would consider usual, it's worth asking why.

Does the offer come with pressure to change your services, messaging, or public positions? If the offer is tied to your organisation altering what you do, say, or stand for, it could be an attempt to undermine your organisation's independence.

An international visit sounds exciting, but is the offer too good to be true? Attempts at foreign interference are more effective when on "home ground". Do your due diligence on your destinations to understand any associated risks.

Is there pressure to reciprocate? The offer may come with a caveat of needing to return the favour. While this may align with the community organisation's values, it could be used to apply unwanted pressure.

Have a clear, agreed process and next steps in place for what to do if concerns about gifts, funding donations or favours are identified.

This content is based on information from the Protective Security Guidance resources.
This information is intended to provide general guidance and promote understanding.

About the due diligence tool

Key steps for your due diligence process

What is due diligence for community organisations?

Due diligence is designed to identify potential risks facing your organisation, including foreign interference risks. It is the process of gathering information about individuals or organisations before forming any connections, partnerships or engagement. However, not all risks may be identified through due diligence. Many organisations already carry out steps like vetting and police checks, but due diligence can gather additional information from the public domain to better understand people and organisations.

How to approach it

You can use publicly available sources to gather information – see the next pages.

The goal isn't to uncover every detail but to identify any obvious risks and ensure you're comfortable moving forward.

By staying curious and cautious, your organisation can build stronger, safer relationships that benefit your organisation and community.

How to use it

While due diligence is an important part of minimising risk there will always be limitations to the information you can access.

Due diligence should be viewed as a tool to help you make more informed decisions, not as a guarantee against all risks.

If you encounter situations where you're unsure or feel you lack the expertise, consider seeking external advice, whether from legal professionals, experts in nonprofit governance, or authorities.

Key things to remember

- **Talk to trusted contacts**: Reach out to trusted individuals who may have a relationship with the new individual or organisation to learn more.
- **Ask clear, direct questions** when engaging with a new individual or organisation about their background, funding, or any potential conflicts. Transparent partners will be open to these conversations.
- **Trust your instincts:** If something feels off or inconsistent, seek more information before moving forward. You can always say no if you feel uncomfortable.

The role of leadership

Due diligence is the process of gathering information about individuals or organisations before forming any connections, partnerships, or engagement. To ensure this is effective, it's important to clearly identify when, where and how due diligence should be applied within your organisation's operations. Leadership plays a key role in understanding these needs.

How to use the due diligence tool

Key steps for your due diligence process

How to use this tool

This tool highlights key steps when carrying out due diligence on individuals or organisations. It can be used as a checklist or a conversation guide. Depending on the situation, additional and more specific inquiries may also be needed.

Overseas connections and networks

When doing due diligence remember: many people, especially from ethnic communities, naturally have legitimate overseas connections and networks outside of New Zealand. This doesn't automatically mean there's a risk of foreign interference. **See:** Information about foreign interference.

More information about due diligence

See Protective Security Guidance: Due Diligence Assessments - For Espionage and Foreign Interference Threats and Managing Inwards Visits. It contains principles and more advice that can help strengthen organisations' overall risk assessment processes.

Check	For individuals	For organisations
Who are they?	❑ Verify full name, location, and professional background (use LinkedIn, personal websites, etc.). ❑ What do their profiles or website tell you about career history, previous roles, and affiliations? ❑ Identify past employers and current affiliations via background and reference checks. ❑ Have they disclosed any partnerships with foreign groups or governments? ❑ Do online searches for their name, nicknames, and any known associated companies, organisations, international affiliations or networks. Look for news articles, social media profiles, and any other relevant mentions.	❑ Confirm their legal status (registered charity, company, nonprofit, etc.) ❑ Is the organisation registered with the Companies Office or Charities Services? ❑ Has the organisation disclosed any partnerships with foreign groups or governments? ❑ How is the organisation funded? Are any funding sources linked to foreign governments or entities? ❑ Do they disclose their major donors and partners? How transparent are they about this? ❑ Do online searches to identify any connected companies, organisations, international affiliations or networks. Look for news articles, social media profiles, and any other relevant mentions.
What network groups or associations are they part of?	❑ What professional, community, or industry groups do they belong to? ❑ Consider how these memberships might shape their reputation, extend their network, or influence their standing within relevant circles.	❑ What professional, community, or industry groups is the organisation connected with? ❑ Consider how these memberships might shape their reputation, extend their network, or influence their standing within relevant circles.

Continued on the next page

How to use the due diligence tool

Key steps for your due diligence process

Check	For individuals	For organisations
Who follows and engages with them online?	❑ Take note of the types of followers and connections they engage with online. ❑ What do their followers and interactions tell you about the strength and reach of their connections and influence within their community or sector?	❑ Take note of the types of followers and connections they engage with online. ❑ What do their followers and interactions tell you about the strength and reach of their connections and influence within their community or sector?
What do they say publicly?	❑ What public statements, interviews, articles, or speeches are available from them? What do these show about their values, priorities, and approach? ❑ How do they express their viewpoints, and what tone or style do they use in their communication? ❑ What do their social media profiles (LinkedIn, X (Twitter), Facebook etc) and website tell you about their interests, values, and affiliations? ❑ How do they present themselves publicly? What topics or causes do they engage with? ❑ Search for the person in news aggregators and databases like Google News. Look for any mention of them in articles, press releases or online media.	❑ What public statements, interviews, articles, or speeches are available from them? What do these show about their values, priorities, and approach? ❑ How does the organisation present its viewpoints publicly, and what tone or style do they use in their communication? ❑ Review organisations social media and website for interests, values, and affiliations. ❑ How is the organisation publicly represented? What issues or causes do they focus on? ❑ Search for the organisation in news aggregators and databases like Google News. Look for any mention of them in articles, press releases or online media.
What is their reputation and what do references say about them?	❑ Reach out to organisations, contacts, or stakeholders who have experience working with them to learn more about them. ❑ Are there any concerns raised by those who have collaborated with them in the past? ❑ Do references suggest they maintain independence and integrity in their work? ❑ Do an internet search to look up the individual's name together with words such as "reviews," "complaints," or "scams."	❑ Reach out to organisations, contacts, or stakeholders who have experience working with them to learn more about them. ❑ Are there any concerns raised by those who have collaborated with them in the past? ❑ Do references suggest they maintain independence and integrity in their work? ❑ Do an internet search to look up the organisation's name together with words such as "reviews," "complaints," or "scams."
Checking web content	For all internet searches, you could search The Wayback Machine. It lets you access earlier versions of a page, which can help verify information, track changes, or retrieve content that's no longer available online.	

Continued from the previous page

Key practices for strengthening IT and device security:
Checklist for everyone in your organisation

There are four key areas to secure

- **Wi-Fi**
- **Passwords**
- **Devices**
- **Accounts**

Secure your Wi-Fi

Your Wi-Fi network is a potential access point for malware and virus attacks. To help keep your organisations Wi-Fi network safe:

- ❑ Make sure your Wi-Fi network names do not reveal information about your location or your network equipment.
- ❑ Set up a password to protect your Wi-Fi, so people outside your organisation cannot access it.
- ❑ Create a guest Wi-Fi network with a password protected connection and separate from your organisation's main network, to prevent potential malware or viruses from guests' devices from affecting the main network.
- ❑ Change the default administrator name and password of your router, to make it harder to access.
- ❑ Check your router for firmware updates as they will help keep your security settings up to date. Schedule automatic updates (if available). Create a schedule or reminder to restart your router every month.
- ❑ Enable a firewall on your router to help stop malware or virus attacks.

Secure your passwords

Weak passwords can increase your risk of malware and virus attacks.

- ❑ A strong password is long (at least 16 characters), has multiple characters and symbols in it, and is not reused across multiple accounts.
- ❑ If your passwords are not already long and strong, update them.
- ❑ You should start with your most important accounts as a priority, but make sure you update all passwords as soon as you can.
- ❑ Change your password if you have any suspicion your devices or accounts have been compromised.
- ❑ Install a multi-factor authentication (MFA) to add another layer of protection to account and device access.
- ❑ Check that all your accounts that support MFA are configured to use MFA.
- ❑ Consider installing and using a password manager and make sure your password manager has your updated passwords.

Key practices for strengthening IT and device security:
Checklist for everyone in your organisation

Secure your devices

Your electronic devices (phone, tablets and laptops) can be vulnerable to online cyber security threats. To help keep your devices safe:

- ❑ Turn on a PIN or password for all your devices. See **secure your passwords.**
- ❑ Enable auto-updates on your devices (phone, tablets, laptops and PCs).
- ❑ Run a full scan of your anti-malware/anti-virus software. Schedule re-occurring weekly updates and full weekly anti-malware scans.
- ❑ Review your mobile application privacy and security settings to make sure these are active and up to date.
- ❑ Turn off your mobile devices daily as this can reduce malware or virus attacks which rely on repeated attempts.
- ❑ Consider using a virtual private network (VPN) service as it hides your Internet Protocol (IP) address and encrypting data, as well as protecting against malware or virus attacks.
- ❑ Make sure passwords on your devices are strong.
- ❑ Apple iOS users - Turn on Lockdown Mode for extra protection.
- ❑ Android users - Ensure you are using Google Play Protect.
- ❑ Consider using a power bank when away from home, or a USB data blocker at public charging stations, to reduce the risk of malware being transferred to your device.

Secure your accounts

Use good security practices to help keep your accounts secure and check they haven't been compromised.

- ❑ Check to see if any of your accounts have been compromised using the Have I Been Pwned Website.
- ❑ Review all your accounts and configure privacy and security restrictions to ensure only the appropriate people have access.
- ❑ Create a full list of all your online accounts so you can keep track and record when each one was last reviewed or updated.
- ❑ Enable multi-factor authentication (MFA) to add another layer of protection to accounts.

More information

More information about staying safe online can be found on the Ministry for Ethnic Communities and the Own Your Online websites.

This content is based on information from National Cyber Security Centre's Cyber Resilience Guidance.
This information is intended to provide general guidance and promote understanding.

How to report to authorities

We can all help keep New Zealand safe from foreign interference by reporting it to the NZSIS or the Police.

Report foreign interference to the Police

If it is an emergency and happening now call 111 and ask for Police

When:

- People are injured or in danger.
- There is a scene or have just left one.
- Serious, immediate, or imminent risk to life or property.
- A crime is being or has just been committed and the offenders are still at the scene.

If you can't talk and you're on a mobile, stay quiet and listen for the 'press 55' prompt; if you're on a landline, follow the operator's instructions.

In a Police non-emergency call 105

If the information is not time-critical, people can report to their local Police by:

- Completing an online report at 105 Police Non-Emergency Online Reporting.
- Phoning the non-emergency number 105.
- Visiting their nearest Police station.
- Calling Crime Stoppers on 0800 555 111.

Report foreign interference to the NZSIS

You can report foreign interference using the secure online form on the NZSIS website.

- You don't have to give your personal information like your name, phone number, or contact details if you don't want to. You can also fill out the form in your own language.
- If you want to talk to someone at NZSIS, you can call them on +64 4 472 6170 or 0800 747 224.
- When the NZSIS sees your report, they will check it. If you leave your contact details, the NZSIS will only contact you if they need more information. If the NZSIS don't contact you, it doesn't mean they have ignored your report.

Reporting foreign bribery

If you suspect foreign bribery, you can report it confidentially through the Serious Fraud Office's anonymous reporting tool.

Learn more: **Report Foreign Bribery - Serious Fraud Office New Zealand**

Report other offences to the Police

Activities such as the ones listed below are offences in New Zealand and should be reported to the Police, regardless of whether they involve foreign interference:

- Blackmail.
- Harassment.
- Intimidation and threats.
- Bribery.

Learn more

Ministry for Ethnic Communities

There are more than 200 ethnic groups in New Zealand but only some are likely to experience foreign interference.

Ethnic communities can receive unwanted and unnecessary attention from foreign states and their supporters.

Resources for communities about foreign interference are available on the Ministry for Ethnic Communities website in 30 languages.

New Zealand Security Intelligence Service (NZSIS)

Each year NZSIS publishes its independent assessment of the threats of foreign interference, espionage, violent extremism and terrorism facing New Zealand.

There is also advice on how to respond if you notice concerning behaviours or activities.

Learn more: New Zealand's Security Threat Environment

Protective Security Requirements (PSR)

PSR have resources and case studies that outline the potential risks for different groups and advise how to protect individuals, organisations, and assets.

Learn more: Resources | Protective Security Requirements