



Te Kāwanatanga o Aotearoa
New Zealand Government

Security advice for Election Candidates

Ensuring your safety and security during
your candidacy for elections

August 2026

Table of Contents

Introduction	2
Privacy Considerations	3
The issue	3
What you can do	3
More information	4
Key contacts.....	4
Personal Security	5
The issue	5
What to do.....	5
Key contacts.....	7
Cyber Security	8
The issue	8
What you can do	8
More information	10
Key contacts.....	10
Foreign Interference and Espionage.....	11
The issue	11
What you can do.....	12
More information	13
Key contacts	13

Introduction

All General Election candidates should understand and consider the potential risks related to privacy, personal security, cyber security, foreign interference and espionage that may arise from standing for election.

The security advice in this document provides visibility of potential privacy and security issues, and to explain mitigations that can be put in place.

This document helps candidates:

- Understand the potential privacy and security issues that may arise
- Know the threat of foreign interference and espionage
- Protect themselves and the people around them
- Know where to go for help and to report incidents.

Contact details and additional resources and links are available at the end of each section.

This advice has been updated for the 2026 General Election.

It was produced by a sub-group of the Major Events Security Committee comprised of:

- Department of Prime Minister and Cabinet
- Electoral Commission
- Government Communications Security Bureau
- New Zealand Security Intelligence Service
- New Zealand Police
- Office of the Privacy Commissioner

Privacy Considerations

The issue

There are various potential privacy risks from election activities that should be considered.

Think about how your information may be exposed to the public:

- Social media accounts
- Cars with election livery
- Election advertising
- Companies register
- Business cards
- Mailing lists.

Having publicly available information about you online could lead to:

- Phishing attempts (including via email or text message) to harvest your login details for personal accounts e.g. banking accounts
- Unauthorised access to online platforms or internal IT systems
- Online scams delivered by messaging platforms such as Facebook, Instagram, or WhatsApp
- Public disclosure of your or your family's personal information
- Other targeting as explained in further detail throughout this document.

Remember that information can remain online for a long time and after the election. Neglected accounts can lead to the same risks happening over the long term.

What you can do

Personal vs public profiles

Public-facing profiles and collateral, on and offline, are a rich source of data and information for those who want to collect it for both legitimate and illegitimate purposes. As a public figure, you should separate your personal accounts completely from your public ones.

- Turn on privacy functions on all your personal accounts (for example, limiting who can interact with you online).
- Consider using a new phone number or PO Box, especially if these are going to be linked to a public profile.
- Create completely separate email and social media accounts for your public campaign.
- Ensure your accounts are protected with long, strong, unique passwords and multi-factor authentication.
- Keep all of your devices' software up to date.
- 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.

Your obligations under the Privacy Act 2020 and protecting the privacy of others

While it's important to keep yourself safe from privacy risks, it's also essential to consider any potential privacy risks to others, and your obligations under the Privacy Act 2020 including how you handle and dispose of information.

Some key things to consider:

- Understanding what voter information you will collect and why, and how you will communicate this to voters
- Provide guidance for staff and volunteers about their obligations under the Privacy Act 2020 when it comes to handling voter data.
- Have a privacy breach plan ready in case of a cyber incident or any other breach of voter information.
- Implement a data retention policy if party officials or volunteers are gathering information about voters. This should include how that information will be held, when it will be disposed of, and then how it will be disposed of.
- Ensure you know who your appointed privacy officer is.
- Following the cyber security guidance later in this document to make sure you are taking steps to safeguard the personal information you hold.

More information

For more advice visit the [Office of the Privacy Commissioner website \(privacy.org.nz\)](https://www.privacy.org.nz).

Key contacts

AGENCY	PURPOSE	CONTACT
National Cyber Security Centre (NCSC)	General enquiry	info@ncsc.govt.nz
	Report a cyber incident	Report an incident and request support National Cyber Security Centre 0800 SIS 224
Office of the Privacy Commissioner	Further information about privacy and elections	Information about privacy at the 2026 General Election (for voters, candidates and volunteers)
	Make a privacy complaint	Complain to the Privacy Commissioner

Personal Security

The issue

As a candidate standing for election, you will be held to a higher standard to ensure the safety of yourself, your supporters, and the public.

What to do

Personal security considerations

- While you are a candidate you will need to have a heightened awareness of your personal and physical security. This will continue if you are successful in being elected.
- Your personal security and that of your team will depend on planning, maintaining situational awareness, and making informed decisions. Be aware of your surroundings and personal safety at all times and when in public, know where you are travelling, who is travelling with you, and how you can exit a location if you need to leave quickly. Consider travel arrangements and how you will mitigate associated risks.
- You are likely to be recognized and approached, and some members of the public may be unpredictable in their actions and behaviour. Consider how you would leave a conversation with someone who has approached you with poor intent; having a robust security plan allows you to engage confidently while also being prepared to expect the unexpected.
- Consider the security of your home and workplace. If you have security controls in place already, check they are working and whether they need to be updated.
- Be aware of the information you make public. Your contact information, personal details, location of personal vehicles, and other information will be readily available to the public through signage, public databases, and social media.
 - This applies to family, supporters and close friends whose information may be accessible through your own personal profile. Remind them to reassess the accessibility of their personal information.
- Consider the contact details you will include in any election advertising you initiate, and create separate contact information (like emails or PO Boxes) to use for public-facing material. All election advertising must include a promoter statement with the name and contact details of the person promoting the advertisement. You don't have to include your street address. Contact details can be one or more of the following:
 - the person's address
 - the person's email address
 - the person's post office box number
 - the person's phone number
 - a link to a page on an internet site that contains one or more of the person's above contact details.

- Consider seeking professional advice to assess your individual security requirements.

Personal security at events

Hosting an event

As the organiser you have a responsibility to ensure your safety, the safety of attendees, and safety of the public. Pre-planning and having a safety-first mentality are crucial to a safe and successful event.

Before the event

- Always pre-book a location you intend to use, as others using the space may impact your event.
- Utilise traditional media, social media and local connections to scope prospective and venues.
- Visit the site beforehand to learn more about the venue and ensure it is appropriate.
 - If you have booked a private venue, meet with the building/location venue manager ahead of time.
 - If the event is being held in a public place speak with the local council or appropriate local administrative body about your plans.
 - Speak with appropriate venue staff about evacuation plans should a natural disaster event or other unplanned threat occur.
- Ensure you and your support staff are aware and familiar with the safety plan for the venue.
- Plan entry and multiple exit points in advance should you need to leave quickly.
- If you anticipate the event may affect pedestrian or vehicular traffic speak to your local council about implementing a traffic management plan.
- Consider visiting the site immediately before your event and have a contingency plan if you have a safety or security concern.
- Have a plan in place should protestors attend and disrupt your event.
- Consider engaging security guards as a further prevention measure to enhance safety for all attendees.

During the event

- Provide a safety briefing covering the evacuation process and rally point at the start of your event. This will ensure all participants are informed and will aid a more effective response if something does happen.
- Secure all personal belongings or have them looked after by support staff. Don't leave valuables, personal items, or sensitive information unattended.
- Make sure all signage complies with local bylaws and doesn't become a hazard or obstruction for pedestrians and vehicles.
- If you or your supporters are driving to the event, park in a location that is safe and easy to access if you need to leave quickly. Ensure your vehicle is locked, and you have a spare set of keys readily accessible.

Communications

For all events you participate in, either as a host or attendee, make sure you have:

- A working and tested communication plan.
- Charged your phone and checked it is functional
- Contact information of your support staff
- Tested your event location has adequate reception and/or data connection.

Nominate a safety person/s who can act should an emergency happen. They should know:

- Your itinerary
- The event location and duration
- Key personnel and their contact information
- Your emergency contact to notify in an emergency.

More information

For more safety advice visit:

- <https://www.police.govt.nz/advice-services/personal-and-community-safety> (police.govt.nz)
- <https://www.police.govt.nz/advice-services/protecting-crowded-places-attack> (police.govt.nz)

Key contacts

AGENCY	PURPOSE	CONTACT
New Zealand Police	In an emergency	Call 111 in an emergency
	Report an incident	If an incident has already happened and there's no immediate danger, call 105 or visit <i>105 Police Non-Emergency New Zealand Police</i>

Cyber Security

The issue

As a candidate you will be interacting with more people online than usual, which may present an increased risk. The volume of information you share publicly can make you more vulnerable to targeted, sophisticated attacks. You should consider the advice below and ensure you have taken steps to secure your information online. You can also use the NCSC's "[How Exposed Am I](#)" tool, which shows if your personal information has been leaked online and offers guidance on protective actions.

For further guidance see [Own Your Online](#) and the NCSC guidance for high profile individuals here: [Cyber security guidance for high-profile individuals \(ncsc.govt.nz\)](#).

Good cyber security practices help you protect the things and people that are important to you. While there's no fool proof way to prevent a cyber incident or data breach, there are things you can do to help reduce the risk. Start by creating a list to identify and track your digital assets including devices, software, accounts, and platforms.

What you can do

Multi-factor authentication

Multi-factor authentication – also known as MFA – is the simplest and most effective way of securing your online accounts.

After logging in, the MFA system will ask for an extra piece of information. This is usually a code sent to your phone via text or code generating app (sometimes called a token). On your device it might also be a face ID, fingerprint, or PIN. Other examples of advanced MFA include physical tokens (such as YubiKeys, Google Titan keys, or FiDO2 keys).

This means even if your password is leaked, there is still a second level of protection.

We recommend having MFA on wherever you can. This includes your devices – laptops, tablets, smartphones – and your online accounts:

- Email
- Social media
- Internet banking.

Strong, unique passwords

Having a strong and unique password for each of your accounts is solid start for anyone wanting to increase their cyber security.

- **Make your passwords long and strong:** A long unique password for each account seems like a lot of work but it pays off. If your password is leaked in a breach, or otherwise discovered, then you know attackers can't use it to get into any other accounts.

- **Don't use personal information to create your passwords:** Passphrases – four or more random words in a string with special characters and numbers – are a good way to create memorable passwords that are tough to crack (for example: RainingDalmations&17KakarikiCatfish).
- **Use a different password for every online account you have.** Doing so ensures that if one of your passwords is leaked or otherwise discovered, it cannot be used on any other account.
- **Use a password manager to store complex passwords:** A password manager is a good way to keep all those long passwords organised; all you need to remember is the password to get into the manager. Some systems have built-in managers, such as Apple and Google, but there are also a range of other password manager apps available. You can also consider writing them down in a notebook and keeping that in a secure location. The 'remember my password' feature offered in some browsers is not as secure as a dedicated password manager, and we recommend against using it.

Keeping your devices secure

Most people run their lives through digital devices and it's vital to keep them secure.

- **Turn on automatic updates:** ensure you're updating your devices with new software. Sometimes the purpose of these updates is the release of a new feature, but often they are about fixing weaknesses or vulnerabilities on your device.
- **Physically hold on to your devices:** losing a device is a common way for data or credentials to be compromised – so keep them safe. Do not give out your device's login passwords and ensure you have location and tracking services enabled. This will also allow you to remotely wipe it in an emergency.
- **Don't connect unknown devices:** malware can be delivered by removable media like USB sticks. This includes public USB charging stations, which may be compromised by cyber criminals. If you are given or find a USB device, do not use it. Hand it to a security professional to ensure it's safe.
- **Avoid using unsecured Wi-Fi networks:** this includes in hotels, airports, cafés or other public spaces. Enable mobile data when you're not connected to a trusted network.

Separate personal and professional accounts

Social media accounts have become a rich source of data and information for those who want to collect it for both legitimate and illegitimate purposes. As a public figure, you're advised to separate your personal accounts completely from your public ones.

- **Turn on privacy functions** on all your personal accounts (limiting who can interact with you online).
- **Create completely separate email and social media accounts** for your public campaign.
- **Consider getting a separate phone number** for sharing with the public. Using a separate email for managing key services like banking is also recommended.

The most important online asset you have is the email account that password reset links go to when you have forgotten your password. Ensure this email account is protected with all the advice above.

Keeping your personal accounts locked down will help keep private knowledge out of the public sphere. It is important to understand your existing data footprint and what information may already be available, for example, through historic data breaches. The NCSC's "[How Exposed Am I](#)" tool can help to identify any exposure.

Remember that these accounts will exist after the election. Consider deactivating the public accounts if they aren't needed but *not* deleting them – this means no one can take the username afterwards and pretend to be you.

Accounts which require multiple users should have individual login details to track user activities, and strict access limitations.

More information

- [Protect your business with two-factor authentication \(2FA\)¹ - \(ownyouronline.govt.nz\)](#)
- [Create good passwords - \(ownyouronline.govt.nz\)](#)
- [Use a password manager in your business - \(ownyouronline.govt.nz\)](#)
- [Keep up with your updates - \(ownyouronline.govt.nz\)](#)
- [Stay safe on social media – \(ownyouronline.govt.nz\)](#)
 - [Setting up your business social media securely - \(ownyouronline.govt.nz\)](#)
- [Secure your home network - \(ownyouronline.govt.nz\)](#)
- [Cyber security guidance for high-profile individuals \(ncsc.govt.nz\)](#)

Key contacts

AGENCY	PURPOSE	CONTACT
National Cyber Security Centre	General enquiry	Info@ncsc.govt.nz
	Report a cyber incident	Report an incident and request support National Cyber Security Centre 0800 SIS 224
New Zealand Police	Report an incident	Call 105 or visit <i>105 Police Non-Emergency</i> <i>New Zealand Police</i>

¹ This will be updated to Multi-Factor Authentication guidance in October 2026.

Foreign Interference and Espionage

The issue

Foreign states may target you to advance their goals in ways that undermine New Zealand's sovereignty and national security.

Foreign interference is an act by a foreign state, often through someone working on its behalf, intended to influence, disrupt, or subvert New Zealand's national interests by deceptive, corruptive, or coercive means. There are two main forms: political and societal.

- Political interference may target governance systems (including the electoral process), the information environment, and politically influential people.
- Societal interference may target individuals, communities, businesses, social and activist groups or the information environment.

Espionage, or spying, is covertly accessing non-public information. The information sought could hand a foreign state, or its proxies, valuable insight into you or your political party that could provide the foreign state with a strategic advantage.

This guidance is designed to make you aware of these risks and how they might affect you and your staff. Further information can be found in the [New Zealand Security Threat Environment Report \(nzs.govt.nz\)](https://nzs.govt.nz/publications/new-zealand-security-threat-environment-report).

Why might you be targeted by a foreign state?

You and your staff are of interest to foreign states.

In your role, either as a candidate or elected official, you are in a position of influence with access to a wide range of sensitive information. Your ability to steer policy and your access to other people in positions of power could make you an attractive target. New Zealand's position on international issues and our international relationships may also be of interest. There may also be particular political issues you hold views on that are sensitive to a foreign state which wants to amplify or undermine these.

How might you be targeted?

Many interactions with foreign intelligence services or those working on their behalf, will seem like normal networking opportunities. Foreign intelligence services often use third parties to conduct foreign interference; these could include diplomats, academics, business people, military personnel, and media organisations. Foreign states also use front organisations to shape New Zealand's social and political environment, including by taking control of community organisations and replacing authentic and diverse community views with those approved by the foreign state.

There are a range of ways you may be targeted, from attempting to draw information of value through targeted conversation, to more technical methods, such as interfering with your electronic devices or using cyber exploitation. Targeting may occur in-person or online, for example through professional networking and job recruitment sites. You may be directly asked or unwittingly used by foreign

interference actors to support foreign state narratives or suppress views and activities that are unfavourable to the foreign state.

Why should you care?

Any influence a foreign state actor manages to apply over New Zealand's Parliament or other elected bodies could damage New Zealand's democratic process, subvert our sovereign decision making, undermine New Zealand's commercial edge over a competitor, compromise negotiating positions, or damage our national security. Moreover, there is potential your reputation, the reputation of your party, or New Zealand could be negatively impacted. You could also be put in a position which leaves you open to pressure or coercion.

What you can do

Keep yourself safe

Approaches by foreign state actors are unlikely to be obvious, however the advice below will help protect you and your staff from becoming subject to foreign interference and espionage efforts:

- **Be vigilant:** is their interest unusual or persistent given your normal interactions? Look out for SOUP approaches: **S**uspicious, **O**ngoing, **U**nusual or **P**ersistent.
- **Check their identity and connections to foreign governments:** research any unknown individuals online and check whether the organisation they represent exists.
- **Take a trusted colleague with you when meeting someone new:** having a third party at a planned meeting can deter these types of approaches
- **Ask how your photo will be used:** it is reasonable to require your approval before someone shares your photo online, including the tagline, to ensure your image is not misused and your views are not misrepresented.
- **Conduct due diligence on any offer you receive:** donations and gifts (including meals and travel) are used by foreign states to build influence and leverage in New Zealand's democracy. Ensure you comply with transparency rules and legislation. You can say 'NO.'

Report concerning behaviour

If you believe you have been targeted, have experienced a SOUP interaction, or want to report concerning behaviour, please report it to the New Zealand Security Intelligence Service at nzs.govt.nz.

SOUP behaviour may look like:

- being asked for official information that a person does not need to know
- being asked for information about the people you are working with
- being encouraged to establish ongoing contact about official matters outside of official channels
- being offered hospitality or gifts and encourage not to tell people about them
- receiving an unusual degree of interest in your work or personal life
- receiving a pattern or a degree of persistence that doesn't feel right.

Recognising and reporting concerning behaviour helps you manage the risk and helps keep you safe. Concerns do not have to be major, something that feels minor to you may be a piece of a larger picture.

Other mitigations

While this advice serves to raise your awareness of the risks and provide advice for you to protect yourself and those around you, there are other mitigations that are also in place.

Foreign interference is now a criminal offence. This means that should criminal thresholds be met, New Zealand Police may seek to pursue charges and prosecution. In addition, the Ministry of Foreign Affairs and Trade have briefed the diplomatic and consular corps in New Zealand on acceptable and unacceptable behaviours from their offices over the election period. This includes how they engage with candidates, political parties and communities – noting that action can still be taken despite diplomatic immunities.

Please report concerning behaviour to enable agencies to take appropriate action.

More information

- For more information on national security threats please see the [New Zealand Security Threat Environment Report \(nzsis.govt.nz\)](https://nzsis.govt.nz).
- For more information on foreign interference in different languages visit the [Ministry of Ethnic Communities website \(ethniccommunities.govt.nz\)](https://ethniccommunities.govt.nz).
- For more protective security information, go to www.protectivesecurity.govt.nz (protectivesecurity.govt.nz).
- For more detail on how you may be targeted and ways to keep yourself safe, read the Protective Security Requirements resource [Espionage and Foreign Interference Threats: Security Advice for members of the New Zealand Parliament and Locally Elected Representatives \(protectivesecurity.govt.nz\)](https://protectivesecurity.govt.nz).

Key contacts

AGENCY	PURPOSE	CONTACT
New Zealand Security Intelligence Service	Queries on this content, or requests for engagement	engagement@nzsis.govt.nz
	Report concerning behaviour or an incident	NZSIS public reporting form here (nzsis.govt.nz) 0800 SIS 224 (0800 747 224)
	Stay informed on national security threats	Visit the NZSIS engagement page here (nzsis.govt.nz)
New Zealand Police	Report an incident	Call 105 or visit <i>105 Police Non-Emergency / New Zealand Police</i>