Government
Health & Safety Lead

Keeping yourself safe

A guide to personal security

New Zealand Government

Contents

Introduction

This guide is intended to provide you with practical steps you can take to protect personal information (such as where you live) from potential threats. It provides some useful guidance on how to go about taking some basic steps to protect your private life from unwanted approaches, particularly from clients who you may work with.

Not all staff will want or need to take all the steps in this guide. It's about assessing the risk for you and taking what action is proportionate and sensible. This might change from time to time in response to risk or due to the nature of your work at the time. You should also consider seeking advice where necessary.

Some government agencies will have their own guides for the personal safety of staff based on their particular risk profile. This guide is not intended to replace any agency specific guidance.

Serious imminent threats should be managed through your agency's security policies and procedures and, depending on the seriousness of the issue you may also need to involve the Police.

Who should protect their private information?

For most government workers it is generally not necessary to take the steps laid out in this guide; however, any person who is concerned about their safety or the safety of those closest to them should take some basic steps to protect their private information.

The following groups of people should consider taking basic steps to protect their private information:

> Chief executives and other senior leaders
> Government workers directly involved with controversial policy issues or exercising decision making powers that directly affect individuals (ie case managers etc)
> Any government worker who is threatened or has become the target of fixated individuals.

It is also important to consider how you handle identifying information about other employees within your organisation when responding to official information or privacy requests. This could include, but is not limited to the release of DDI's, mobile numbers, email or physical addresses by reception staff.

Some basic sources of public information about individuals

There are a number of publicly-accessible records that can be used to match your name with other personal information such as your home address, family members' details, and private phone numbers.

These records include:

> social media
> electoral roll (which can contain details about a person's home address and, potentially, others residing at a person's home address)
> telephone records (which may have home phone number and address details)
> vehicle ownership details (which contain details about car and residential details)
> property details
> company, trust or charity records.

You should be aware that while it is reasonably easy to protect certain personal details in these records, it is difficult to achieve perfect anonymity.

A determined individual can take more advanced steps such as locating historical information or commissioning research through professionals such as private investigators or credit reporters. In the digital age, once information is online, it will usually remain there unless you can have it removed or changed.

Social media

Online social networking is a great way to stay in touch with friends and family but think about what you're posting and who could see it.

Tips for safe online use of social media:

- Avoid posting anything that shows where you work – disgruntled clients may target you because of where you work, even if they don't know you.
- Avoid posting personal information, for example dates of birth, maiden names, names and details of children etc.
- Think carefully before accepting friend requests – is the person really a friend? (If you're not sure, it's OK to ignore the request).
- Use privacy controls on sites like Facebook so only approved users can view your page.
- Restrict who can share information and photos you have posted to your page so other users cannot forward your information.

There are no guarantees of privacy, even with tight security settings. Anything you put on a social networking site can be cut, pasted, or sent simply by taking a 'screen shot'.

Photos are often 'tagged' so that the names of the people in the photo are given. This can violate the privacy of the people linked to the photo. In the security settings of social networking profiles, ensure that where possible other users are restricted from being able to 'tag' individuals in photos they post to their own accounts.

When using social networking sites on smart devices (such as iPhones or iPads), users can 'check in' to locations, which simply shows where they are, eg a particular restaurant. Others can use this type of information to track down the user.

Photos taken on smart devices are often automatically geo-tagged (geographical data is imprinted into the photo properties which shows where the photo was taken). When these photos are uploaded to social networking sites, this data often remains. If a user has uploaded, for example, a photo of their new house extension or vegetable garden, someone could potentially use the geo-data embedded in the photo to obtain the user's home address.

Talk to family, especially children, about staying safe online and as part of that, discuss the importance of not revealing personal or professional information about a government worker online without explicit permission.

www.netsafe.org.nz has some good guidance available around cyber security, scams, protecting your identity and general safety online.

Electoral Roll information

Being enrolled to vote means that your name, address and occupation can be viewed by anyone who looks at the printed electoral rolls. These can be viewed in many places, including most public libraries and PostShops.

If you are concerned that having your details recorded on the printed electoral roll threatens your personal safety, or that of your family, you can ask the Electoral Commission to remove your details from the public roll, and have them included only on the confidential unpublished roll.

To apply to go on the unpublished roll you will need to contact the Electoral Commission by the following means:

- Download the unpublished roll application form from www.elections.org.nz
- Call the Commission on 0800 36 76 56.

The unpublished roll is strictly confidential and can only be accessed by a Registrar of Electors and a small number of other Electoral Commission staff. However, it is important to note that older copies of printed electoral rolls may still be accessible to the public.

You will need to cast a special vote if you enrol on the unpublished roll because your details won't be included in the printed roll used to issue votes at the voting place in a General Election or by-election. For local council and DHB elections, you will need to contact the electoral officer at your local council to receive a special vote.

Vehicle registration and registered person name and address details

If a vehicle is registered in your name, your name and address details are recorded by the New Zealand Transport Agency (NZTA) on the Motor Vehicle Register.

Anyone can apply to get a registered person's name and address (MR31). However, the personal information NZTA holds on the register is protected by privacy laws. Each application is considered under section 237 of the *Land Transport Act 1998* and the criteria contained in the *Official Information Act*. NZTA must weigh up the public interest in releasing the information sought against the privacy rights of the person concerned.

If you do not want your name and address to be automatically provided you can 'opt-out' by requesting NZTA hide your details. This means the release of information needs to be considered on a case by case basis by an NZTA staff member.

There are a number of people or organisations that have a legitimate need to access the Motor Vehicle Register, such as insurers, finance companies and motor vehicle traders. Opting-out could mean it will cost more and take longer to complete transactions with these organisations as they will be required to specifically request this information from NZTA.

You can find information on opting-out at:
transact.nzta.govt.nz/transactions/PersonalInfoAccess/entry

Note:

> To opt-out you will need your New Zealand driver licence and vehicle plate number(s).
> NZTA will also automatically withhold details of any person(s) recorded as a joint registered person if the primary registered person opts-out.
> Opting-out is only available to individuals.
> If you want to opt back in at a later date, you will need to contact NZTA (see www.nzta.govt.nz/contact-us).

You can do a lot online now.
Check out the extensive list at
www.nzta.govt.nz/online-services

Phone details

If you have a landline telephone number, your name, address and phone number will automatically appear in your local telephone directory, as well as the online White Pages. Directory Assistance (dial 018) may also give out this information.

To protect telephone information you have two options:

1. **Confidential (a restricted number)** – This means your name, address and telephone number will not be included in the White Pages and will not be given out by Directory Assistance.
2. **Non-published (an unlisted number)** – This is an alternative to a restricted number. It means your name, address and telephone number will not be included in the White Pages, or any directory listing on the internet. However, the telephone number will still be given to anyone who asks for it from Directory Assistance. The address will not be given out.

You should ideally only use a work phone for making work related calls. If you are using your own phone, you may wish to get it set up so your number is withheld from services such as Caller Display. Most mobile phones allow you to stop your number being displayed; you should check your mobile's user manual or contact your service provider to find out more about how to do this.

If you do receive threatening or harassing phone calls, you should report these immediately to your phone company and the Police. You should also advise your organisation's Chief Security Officer so there is organisational awareness of what is going on.

NZ Companies Office and Trusts

If you or your family registers a company/business or a Trust in New Zealand with the New Zealand Companies Office, any information you supply about the entity is included in the New Zealand Companies Register.

This is an electronic register where company information and related documents can be viewed online. This includes directors' and shareholders' names and addresses, the registered office of, and address for service of each company. Even when details are updated, previous details are still available for viewing within old paperwork which has been submitted and uploaded to the register.

This information is freely available on the Companies Register. Access to register details is also publicly available online www.companies.govt.nz/cms

The website allows people to search either for an individual or company name. The search result includes details of addresses given at time of registration. The website also holds information for old or disestablished companies.

If you are registering a business or Trust, you can ask the legal/accountancy firm that is involved in the setting up of the company if you can use their business address as the registered office of the company (instead of your own personal address).

If you have already set up a company or Trust with personal details recorded, you might want to consider changing, where possible, names or addresses. While the previous information will still be available, this historical information will be slightly harder to find if it is not on the front-facing information within the register.

Property ownership details

Local councils

Local councils have publicly available Rating Information Databases (RIDs). These databases hold rating information about addresses – including property owner details.

Anyone can visit the council offices and find out the owner and postal details for a specific property. This information is also available on websites such as Quotable Value New Zealand (QVNZ), where for a small fee anyone can request property ownership details by querying a specific address.

If you own (or are the rate payer for) more than one property, you will need to approach all the councils for all the properties.

Some RIDs are online, but these do not usually give access to owner's details and postal addresses.

To keep your details confidential on a RID:

1. Go to your local council's website and check to see if they have a link to the RID database (usually found somewhere in the rates section and may also be called 'property search'). Do a query on your property and fill in and submit the section on non-disclosure and confidentiality of your name and postal details, or submit online the withholding details form, or
2. Go to your council office and make a direct application to the council for non-disclosure and confidentiality of your name and postal details on the RID database.

Land Information New Zealand

Land Information New Zealand (LINZ) holds the Titles Register which contains all property ownership details. LINZ is legislatively bound by statute to disclose property ownership details upon request.

The only legislative authority LINZ currently has to restrict information on their register is under the *Domestic Violence Act 1995*, which would require a person to present a domestic protection order.

There is an administrative process available to hide landowner information where there is an imminent threat to someone's safety, where they cannot or choose not to use the domestic violence regime processes for having identifying information hidden in registers. LINZ requires independent evidence verifying this threat such as confirmation from an employer or the Police.

Recent changes under the *Land Transfer Act 2017*, which comes into effect in November 2018, will provide LINZ with legislative grounds to withhold information for a person's safety. You would still be required to present evidence from your employer or the Police as to why removing your details is necessary.

In all of the above instances if the Registrar agrees to hide a title, it will be for a period between one to five years. This will enable you to seek independent legal advice on other forms of ownership that will keep your identity off the title (such as having the property held in a Trust).

Physical security

The following pointers are mostly common-sense safety tips that you may already take when, for example, walking to your car late at night.

If you are concerned for any reason the first step is to tell your immediate manager. They will help you assess the risk and, if necessary, create a realistic personal security plan, which may include notifying Police.

Security at work

Who are your colleagues?

Getting to know your colleagues is an easy way to ensure that any strangers who gain access to your workplace are easily identified.

Beware of 'ghosting' – when a person follows behind a staff member and gains access to secure areas by slipping through gates or doors before they close.

On large sites, it is impossible to know everyone, so stay alert and if you see someone unfamiliar check they have a visible ID card. All staff are able to challenge an unknown person and ask to see proof that they are allowed to be there – but make sure it is safe to do so. If you are alone you should call for back-up or find a colleague before you challenge someone.

Security outside of work

Out and about

- Tell someone where you are going and when you'll be back.
- If you are walking at night, stay on brightly lit, well-used streets as much as possible. If you must take a poorly lit route, walk near the kerb or well away from shrubbery, dark doorways and other places of concealment. Be 'alert' (take out your headphones) and avoid shortcuts.
- Don't leave anything in view in your vehicle that could associate you with your workplace.
- Park in well-lit areas and always close your car windows and lock the doors.
- Park where you can drive away easily, eg don't park in driveways where your access could be restricted.

Security at home

The suggestions below are ideas you may like to consider in relation to safety at home. You may already be doing many of these.

Family Safety Plan

Think about developing a safety plan for emergency situations that is agreed upon by all members of the household. Every plan will be unique to the circumstances, but here are some important things to consider:

- What will you each do in the event of an emergency?
- How and where will you meet up in the event that the home is no longer safe?
- How will you contact each other in case of an emergency? If you can't contact someone, who or where will you leave a message?
- What will you need to do for members of the household with a disability or special requirement?
- What will need to be done for pets, domestic animals and livestock if the home is no longer safe?
- Who will be responsible for collecting children from school if you need to relocate in a short amount of time?
- Who could help you or where could you go if you need to relocate in a short amount of time?

getthru.govt.nz has some great information and resources on this topic.

Home security

- Always check who is at the door before opening it (consider having a door chain or security peep-hole installed) and never open the door if you are suspicious in any way.
- After dark, close the curtains so people can't look in.
- Check all doors and windows are secure before going to bed, leaving the house (even if you are only popping out for a minute) or going to a different part of the house.
- Keep a strong 'courtesy' light by the front and back doors at night.
- If you go out at night, prepare for your return by turning on outside lights. Some inside lights should also be left on.
- Keep a check on your house keys and never leave one outside in an obvious place (eg don't leave one under the mat or in the letter box).
- Arrange fixed times for trades people to call. Check their identity and never leave them in the house on their own.
- Check parcels/deliveries before accepting them.
- Trim bushes or trees that are close to the house.
- Talk to children and teenagers about staying safe (eg how to open the door or answer the phone).

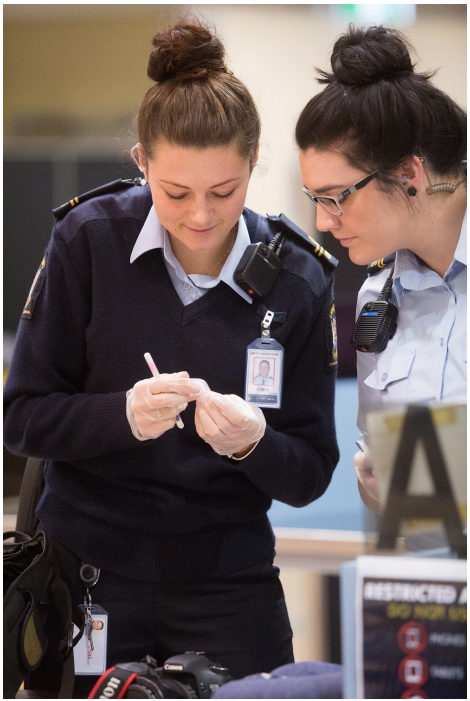
Telephone

- Be wary about giving personal information out on the phone, especially if you don't know the caller. It's better to take a name and number and call back if you are suspicious in any way.
- Make sure children and other family members know to be careful when answering the phone.

Anonymous calls – telephone threats

Anonymous calls and telephone threats are usually intended to lower your morale. Your natural reaction when hearing a hostile voice is one of anger/fear and to cut off the conversation. However, the caller may provide clues to their intentions or specific threats and if possible, you should try to keep them talking:

- Try to identify the voice by age, sex, accent, peculiarities, etc
- Listen for background noise, which may provide valuable information, e.g. music, machinery, animals, industrial noises, railway station sounds etc
- Write down the details of the call immediately
- Contact the Police without delay.



If you receive a threat

If you or a family member receives a threat, this should always be treated as legitimate and serious until proven otherwise.

The first thing to do is:

Consider if it should be escalated to the Police
If a threat is serious, personal and involves a physical threat to you or your family, then you should consider taking the threat to the Police in the first instance.

Talk to your manager.

For more information contact the Government Health and Safety Lead by email on govthealthandsafety@corrections.govt.nz

Government
Health & Safety Lead