community law
free legal help
wellington and hutt valley

# Information & Privacy

## Data privacy and the law

**Privacy Act 1993, s 2**

All organisations, businesses and individuals, whether in the government or private sector, must follow the rules in the Privacy Act. This includes companies and organisations of all sizes, religious groups, schools and clubs. (In setting out the different privacy rules, the Act uses the word "agency" as a general term to refer to all bodies and individuals that have to follow those rules.)

## What does the law say about privacy?

Under the Act, "personal" means that it is information about any individual person, not that it's particularly private or sensitive. If you are going to be collecting personal information there are rules about when you can collect information, how and when that information can be used or given out and requirements about storing the information and keeping it secure.

The Privacy Act has 12 information privacy principles which set out how your agency should handle personal information.

**The first four principles**

Govern how you can collect personal information. This includes when you can collect it, where you can collect it from, and how you can collect it.

- Collecting personal information

**Principles five, six, and seven**

Govern how you store personal information. Make sure it's secure and you let individuals access and correct their personal information.

- Holding personal information

**The rest of the principles**

Govern how you use and disclose personal information. Make sure information is accurate, and you use and disclose it appropriately.

- Using and disclosing personal information

A full guide to the 12 Privacy Principles can be found here.

## Storage and security of information

Privacy Act 1993, s 6, principle 5

If your organisation holds personal information about individuals, you must make sure that reasonable security safeguards are in place to protect the information against:

- being lost
- being accessed, used, changed or released without the organisation's permission
- being misused in any other way.

If your organisation needs to give the information to a contractor or someone else who provides a service to the organisation, the organisation must also make sure everything reasonable is done to prevent the information being used or disclosed without authorisation.

The steps that an organisation will need to take to keep information secure will usually depend on the type of information. For example, an organisation will usually need to protect its databases with anti-virus software, and protect its physical premises from burglary or theft by having a monitored alarm.

## Useful Links and Resources

- CommunityNet Aotearoa provides some great advice below on handling information securely, including how to keep information safe and private and organising your filing system
- The Community Law Manual includes a whole chapter about privacy and information that

may be useful for your community.

- The Privacy Commissioner website outlines how agencies can meet the requirements of the Privacy Act and contains resources and tools to help you in doing so.

## Māori data sovereignty

## What is Māori Data Sovereignty?

Māori data sovereignty is about protecting information or knowledge that that is about (or comes from) Māori people, language, culture and resources. The 'data' in this context refers to information that is digital or digitisable.

The following quote provides context for why Māori Data Sovereignty is important:

> Data from us, and about us and our resources, are valuable assets. Once control of it is lost, it is difficult to regain; Data can be powerful mechanisms for informing and driving Māori/Iwi development at national and local levels but only if we are able to exercise authority over our data.
>
> *Te Mana Rauranga, Pātai*
> https://www.temanararaunga.maori.nz/patai

It is important as a community organisation to understand and work to uphold the principles of Māori data sovereignty. You can read all the principles in full here on Te Mana Rauranga, as well as useful resources and information in relation to the application of these principles.

## Social Media and online safety

Social media has become an essential tool for communication and promotion by community organisations. But it can come with associated privacy risks. One option for community groups to mitigate some of the risks associated with social media is to develop an overarching policy for your organisation. The policy should clearly state what staff and/or volunteers may or may not do on your organisation's social media accounts. Be mindful that the account is a reflection of the values of the organisation.

**Keeping your community safe online**

Netsafe is New Zealand's independent online safety organisation that provides education on preventing online bullying and abuse, scams and security breaches. For helpful tips on staying safe and keeping others safe online, visit their website. Netsafe's resources include information on:

- Online bullying abuse and harrassment
- Preventing ransomware attacks
- Two-Factor authentication
- Emailing hacking
- Backing up your data
- Using a VPN to improve your security

## Accidental spamming

The UEM Act prohibits organisations sending an "unsolicited commercial electronic message" that is commercial in nature. Therefore, if you are sending an email that is for marketing or promoting goods or services, you must ensure that you have the consent of the recipient.

If you do have the consent of the recipient to send the message to them, make sure that you identify yourself clearly within the message itself, how you can be contacted and provide a "functional unsubscribe facility" in the message (so that the person can tell the community venue to stop sending such messages).

## Useful Links and Resources

- Social Media Policy Builder (Ministry for Business, Innovation and Employment)
- Creating a social media policy (TechSoup)