Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Act guidance for landlords and property managers

February 2025

Introduction

As a landlord or property manager, whether you're an individual renting out a single property or a property manager that looks after hundreds of properties, you must collect and handle personal information responsibly and in accordance with the Privacy Act.

Personal information is any information which tells us something about a specific individual. People's names, contact details, financial, health and purchase records can all be personal information. It doesn't need to name the individual, if they are identifiable in other ways, like through their home address or another identifier, or if their identity could be pieced together.

This guidance is designed to help you do privacy well and comply with the Privacy Act. It's not intended to cover:

- public or social housing
- boarding houses
- accommodation that isn't covered by the Residential Tenancies Act 1986, such as certain types of student accommodation and rest homes.

Handling tenants[1]' information responsibly will protect you and them. If you breach tenants' privacy rights, you risk facing a complaint or enforcement action.

The information privacy principles

The Privacy Act is organised around 13 information privacy principles Several of these will be particularly relevant to the collection and handling of tenant information by landlords:

[1] This guidance uses the term 'tenant' to refer to renters at any stage in the rental process, including those who haven't yet been granted a tenancy.

Principle 1: Limits on what information you can collect

You should only collect personal information from tenants if the information is necessary for finding tenants and managing a tenancy. This will vary, depending on what stage you are at in the rental process, and the purpose of collection associated with that stage.

We've produced a guide on the information you can collect for different purposes, at different stages in the rental process. At every stage, you should only ask for the minimum amount of personal information.

When you are arranging property viewings

The only information you should need at a viewing is a person's name and contact details. You can give people the option of completing a full application form before they view a property, but that shouldn't be required at this stage.

When you are receiving applications and shortlisting applicants

You should only ask for the personal information you need to decide whether they're likely to be suitable tenants or not. You can make it optional to answer some

questions, but you still need a good reason to ask them. You must be upfront about any consequences if optional information isn't provided.

You can ask tenants on the application form to consent to a credit check (or a criminal record check – see the discussion of criminal records below) but only carry out those checks once you're negotiating an offer of a tenancy. You can also ask for contact details for landlord and non-landlord referees at this stage and ask the tenants to authorise you to contact these referees, but you should not carry out reference checks at this stage.

To verify an applicant's identity, you could ask to see copies of documents like their passport or driver licence then record the identification number from these. If tenants apply online or by email, and submit images of their identity documents, you should securely dispose of the images once you've completed the verification process (see principle 9).

A pre-tenancy application form is available on Tenancy Services' website www.tenancy.govt.nz.

When you are doing further checks on preferred applicants

More information can be collected from preferred applicants to confirm their suitability for the tenancy, such as contacting referees where necessary to decide about the application.

You can carry out a credit check or criminal record check, with the applicant's consent, when you are actively negotiating the offer of a tenancy. If you decide to obtain a record of a tenant's criminal convictions, you should be clear about how you'll use this information and what convictions you consider relevant.

A key question for landlords is how they can satisfy themselves that the tenant will be able to afford to pay the rent. You must collect no more personal information than is necessary to confirm that the person is a suitable tenant. In addition to a credit report, it should be enough to ask for one other form of evidence of ability to afford the rent, which could include a pay slip or letter from their employer, or evidence of rental payments in a previous tenancy. The tenant should be able to choose which form of evidence they want to provide you.

If the tenant's rent would be paid in part or in whole by an accommodation supplement, the tenant may provide a letter from Work and Income, confirming that the tenant receives the supplement, as evidence of ability to pay the rent.

Except in exceptional circumstances, you should not ask for or collect information about how tenants spend their money: this information will usually be unnecessary and unreasonably intrusive. You shouldn't ask for a full bank statement showing individual transactions, for example (although the tenant could choose to provide a statement showing only the total bank balance). Exceptions could include when a tenant has a negative credit record and wants to show that they've taken steps to improve their financial management; or, once a tenancy has started, when a tenant has become unable to afford the rent and wants to negotiate a repayment plan or rent reduction with the landlord.

When you are preparing a tenancy agreement

Additional information could be collected, such as details of vehicles that will be parked at the property (if necessary for parking arrangements), the tenant's address for service, and emergency contact details. You can also ask for the tenant's Work and Income client number if the rent is being paid using the accommodation supplement, and if you can show that it's necessary to collect the client number to manage the tenancy.

When you are managing a tenancy

Once the tenants start living in the property, you may continue to collect their personal information for the purpose of managing the tenancy. For example, information you collect as part of flat inspections, including photographs of rooms, may be personal information.

When carrying out a flat inspection, you should collect no more information about the tenants than is necessary to assess how well they are caring for the property. When taking photos, you shouldn't include people in the shots or focus on the occupants' personal items unless those items contravene the tenancy agreement. Images containing tenants' personal information that are taken for the purposes of managing a tenancy should not also be used for the sale of a property unless consent from the tenants was sought and given.

Information you should not collect

There is some personal information you should not collect during any stage of the rental process.

Except in relation to certain specific types of accommodation, when choosing tenants, it is unlawful to discriminate based on personal characteristics protected under the Human Rights Act:[2]

- sex (including pregnancy or childbirth)
- relationship or family status
- political opinion or religious or ethical belief
- colour, race, or ethnicity (including nationality or citizenship)
- physical or mental disability or illness
- age (other than whether the tenant is over 18)
- employment status (being unemployed, on a benefit or on ACC)
- sexual orientation or gender identity

There is also other information you shouldn't collect:

- whether the tenants have experienced or are experiencing family violence.
- tenants' spending habits (e.g. bank statements showing transactions).
- employment history.
- social media URLs.

It's unnecessary, irrelevant, and unreasonably intrusive to ask for information about these personal characteristics when you're selecting tenants.

However, once you select the tenant, you may sometimes have a good reason to record information about characteristics such as disability, if it's relevant to how you manage the tenancy (for example, if it affects how you can most effectively communicate with the tenant or respond to their needs).

[2] View more information about tenancy and human rights.

You can collect information about a person's passport for identity verification purposes, even though the passport will also show the person's citizenship. But you shouldn't specifically ask about their citizenship status.

However, you could ask if they have a legal right to remain in New Zealand for the duration of a tenancy that is for a fixed term.

You should not ask people if they have experienced or are experiencing family violence when you are selecting tenants.

You shouldn't ask about tenants' employment history (though you can collect information about their current employment) or ask for their social media URLs.

Principle 2: Limits on who you can collect information from

In general, you should collect personal information about tenants directly from the tenants themselves. However, there are exceptions to this principle.

For example, tenants can authorise you to obtain a criminal record or credit check,[3] or to talk to their referees about them. However, you should only ask for consent to obtain information from specific sources.

You can also collect information about tenants if it's publicly available: for example, if it's on a news website. You need to make sure it's relevant and accurate before using it (see principle 8). It could, for example, be about someone else with the same or a similar name. It could be incorrect or out of date. You also need to use the information in a way that isn't unfair or unreasonable in the circumstances.

You shouldn't assume information is publicly available just because some people are able to view it. A Facebook or other social media profile may be accessible by the tenant's friends and family, but not by the world at large. You shouldn't ask for permission to view social media profiles that are restricted in this way. Seeking or

[3] Credit reporting is governed by a special code made under the Privacy Act. The Credit Reporting Privacy Code allows credit information to be disclosed to a landlord, with the tenant's authorisation, for the purpose of assessing the individual's creditworthiness as a tenant.

requiring access to such personal profiles is unreasonably intrusive on individuals' personal affairs (see principle 4).

You may sometimes need to collect personal information from others during the tenancy. For example, if neighbours complain about the tenants' behaviour, you can collect and record information from the neighbours. Indeed, you may need to collect this information if you're deciding whether to issue a notice of anti-social behaviour to the tenants under the Residential Tenancies Act.

Principle 3: What you need to tell tenants

When you collect personal information from tenants, you need to make them aware of certain matters, such as:

- that their information is being collected (if it's not obvious)
- What information is being collected
- Why it's being collected
- What it's being used for
- Who will receive it
- Whether they must provide the information and what will happen if they don't
- That they can access the information held about them, and they can correct it if it's wrong
- whether the property manager will share the information with the landlord and for what purpose

A common way to meet this requirement is by providing tenants with a privacy statement that explains how you'll handle their personal information. You should include a privacy statement, or a link to it, with your tenancy application form and with your tenancy agreement. Our online tool Priv-o-matic can help you create your own privacy statement.

The privacy statement for your application form shouldn't list purposes for collection that are overly broad or that don't relate to the core purpose of deciding whether

applicants will be suitable tenants. You should also be careful about using the privacy statement to seek consent from the tenants to the collection, use, or disclosure of their personal information: see the discussion of consent below.

Our guidance on creating privacy statements provides further information on what to consider.

Principle 4: Limits on how you can collect information

You can only collect information from tenants in ways that are lawful and fair, and that don't intrude unreasonably on their personal affairs.

What is fair depends on the circumstances, but coercive or misleading behaviour will be unfair. What is reasonable also depends on the circumstances, such as the purpose for collection, the sensitivity of the information concerned, and the time and place it was collected.

For example, it would be unreasonably intrusive to install cameras that could be used to film or record your tenants inside the house or flat they're renting. But it could be justifiable to have security cameras in the public areas of an apartment complex if you have a lawful purpose for monitoring this area.

Principle 5: Keeping information secure

You must keep the information you hold about tenants in a secure system, and make sure it can only be accessed by people who are authorised to do so.

A good starting point is to collect and retain only the personal information you really need (principles 1 and 9). The less information you hold, the less risk there is of sensitive information being lost or misused.

If you have employees, you need to ensure they understand how to handle tenants' information safely. Some employees may not need to access any information or only need to access some tenant information. Your employees must access this information only for work-related purposes. A good practice is to keep property information separate from tenant information, so personal information about tenants can be accessed only by those who need to do so.

The same personal information may be held by more than one agency. If you're a property manager, some information you hold about tenants may also be held by the landlords you work for. If so, both you and the landlord are required to hold the information securely.

If you store tenant information with another business, such as a cloud computing provider, you're still responsible under the Privacy Act for this information. If there's a privacy breach at the agency that is storing information for you, and personal information about your tenants is affected, you'll need to respond to the breach. There's more information about what you need to do when responding to a privacy breach here on our website.

Our guidance on security and internal access controls provides further information on this topic.

Principles 6 and 7: Tenants requesting access to and correction of information

Tenants have a right to ask you for information you hold about them. If tenants request it, you must respond promptly and provide the requested information unless there is a legitimate ground for withholding it. You also need to tell the tenants they have the right to ask for the information to be corrected.

The Privacy Act allows you to refuse to provide some or all the requested information on certain grounds. For example, if releasing it might endanger someone's safety or breach someone else's privacy. If you refuse to provide some information, you must tell the tenant why you've withheld it and let them know they have a right to complain to the Privacy Commissioner.

In most circumstances, an agency should not charge a fee to a requester for accessing or for correcting, their personal information. However, there are some circumstances where it may be appropriate to charge people to access or correct their personal information. Charges must be a reasonable based on the cost of the labour and materials involved in providing the information. We have guidance on charging for personal information.

Before you provide the requested information, you must check that it's going to the right person (the individual whose personal information it is). Check that you have the right email or postal address and have correctly entered or written it.

What information do you need to provide?

Unsuccessful applicants for a tenancy can ask for any information you hold about them, including information that influenced your decision not to offer them the tenancy. If you're asked you should provide copies of all the information you collected for the purpose of deciding on the application, such as:

- the person's completed application form and any supporting documents
- a credit report on the person if one was obtained
- any information you collected from public sources.

You shouldn't provide the requester with information about other applicants to show that their applications were stronger because it isn't information about the requester and providing it would breach the privacy of the other applicants.

You can only refuse to provide the requester with information about them if one of the withholding grounds in the Privacy Act applies. For example, there is a withholding ground for 'evaluative material' that means you may be able to refuse to provide access to a reference that was provided in confidence with the tenant's authorisation. You can find more guidance about withholding evaluative material here on our website.

If current tenants ask for all the information you hold about them, this may include rental payment records, reports of inspections and damage, and complaints received about the tenants.

You don't need to hold on to tenants' information just because they might ask for it one day: you should delete information when you no longer need it (principle 9). If you don't have any information about why someone wasn't chosen, then you don't have to create it. But you must not destroy tenant information after you receive a request for that information: if you do, you'll be committing an offence.

Tenants can ask for information you hold about them to be corrected. You should check the information, and if you agree that it's wrong you should correct it. If you don't agree that the information is wrong, you don't have to correct it. If you are able, you must add a statement of correction to the disputed information if the tenant asks you to. If the information has previously been passed on to anyone else, you need to take reasonable steps to inform them of any corrections you have made or any statements of correction you have added.

Our guidance on responding to requests provides further information on this topic.

Principle 8: Making sure information is accurate

You need to take reasonable steps to ensure the information you use or disclose about tenants is accurate, up to date, complete, relevant, and not misleading.

You only need to take steps to check accuracy that are reasonable in the circumstances. You'll need to consider the source of the information and how reliable the source is likely to be. How old is the information? Is it first-hand information? Is the source likely to be biased?

One way of checking whether information about tenants is accurate, complete, and relevant is to ask the tenants about it. If the information seems to reflect badly on the tenants, you should consider asking them for their side of the story: there may be other information that provides balance or context.

If you're disclosing information about tenants to other people (for example, if you're providing a reference for a tenant with their consent), you should be especially careful not to pass on information unless you're sure it's correct.

Principle 9: Limits on retaining personal information

You should only keep personal information about tenants for as long as you still need it for a lawful purpose. Once you no longer have a good reason to keep it, you should securely dispose of it (for example, shredding paper documents or permanently deleting digital files).

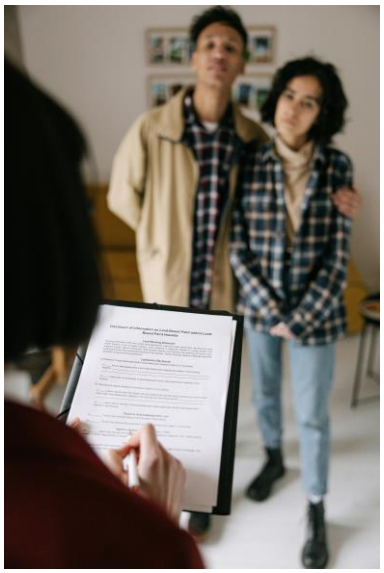
Other laws may require you to keep certain records containing personal information for a specified period. If so, you can comply with those legal requirements without

breaching the Privacy Act. For example, under the Residential Tenancies Act you must keep certain documents during the term of the tenancy and for 12 months after the tenancy ends.

These documents include reports of the landlord's inspections of the property, and correspondence between a landlord and tenants, people to whom the landlord has offered a tenancy, or people who have entered negotiations for a tenancy with a landlord. Landlords also need to keep certain business records, which will include personal information, for seven tax years.

In general, you shouldn't hold on to information about people who have only viewed a property but not applied for a tenancy, or who applied but were not successful. You might want to keep unsuccessful applications for a short period of time in case any issues are raised about the selection process. You can also keep a tenant's application on file if the tenant asks you to retain it, so they don't have to resubmit the information when they apply for another property.

Principle 10: Limits on using personal information



You should generally use the personal information you hold about tenants only for a purpose for which you collected the information, or a directly related purpose. There are exceptions to this principle: for example, you can use the information to deal with a serious threat to health or safety. You can also use the information for another purpose if the tenant has agreed you can do so (but see the discussion of consent below).

Unless one of the exceptions applies, you shouldn't use tenant information for purposes unconnected with the tenancy. For example, you shouldn't use tenants' contact details to promote another business you own, unless they've explicitly agreed to receive such information from you.

Principle 11: Limits on disclosing personal information

You shouldn't disclose personal information you hold about tenants to anyone else, unless the disclosure is for one of the purposes you collected the information for, or another exception applies. The exceptions are like those for principle 10, including that the tenant has authorised the disclosure.

Disclosure can take many different forms. For example, you shouldn't chat to your friends or post information online about your tenants' personal details or behaviour. You should think particularly carefully before making information about tenants more widely available on a webpage or database: see the discussion of tenant 'blacklists' below.

The Privacy Act does allow you to disclose information about tenants to the Police or other appropriate authorities in some circumstances. These circumstances include when you have good reason to think disclosure is necessary to prevent a serious threat to someone's life or health. For example, you could tell the Police if you have evidence that a tenant is making credible threats of harm against others.

Other issues

Privacy breaches

A privacy breach occurs when an organisation or individual either intentionally or accidentally:

- Provides unauthorised or accidental access to someone's personal information.
- Discloses, alters, loses or destroys someone's personal information
- A privacy breach also occurs when someone is unable to access their personal information due to, for example, their account being hacked.

A privacy breach occurs when personal information held by an organisation is:

- accessed, disclosed, altered, lost, or destroyed accidentally or without authorisation, or
- cannot be accessed by the organisation on a temporary or permanent basis. For example, it's encrypted by ransomware; and has either caused, or is likely

to cause, serious harm to someone whose information was affected by the breach.

If your organisation or business has a privacy breach that either has caused or is likely to cause anyone serious harm, it is a notifiable privacy breach and you must notify the Privacy Commissioner and any affected people (unless an exception applies) as soon as you are practically able. A breach notification should be made to our Office no later than 72 hours after agencies become aware of a notifiable privacy breach.

Our guidance on breach management provides information on how to manage a privacy breach.

Complaints handling

If you breach the Privacy Act, you risk a tenant making a complaint to the Privacy Commissioner. The complaint might lead to OPC forming the view that you have interfered with a tenant's privacy. You may have to remedy the breach, such as by paying financial compensation. Complaints that cannot be resolved may be escalated to the Human Rights Review Tribunal.

Our guidance on complaints handling provides information.

We also have a summary document outlining the process for managing a privacy complaint.

When and how you should seek consent from tenants

You don't need further permission to use or disclose tenants' personal information for one of the purposes you collected the information for where you clearly told the tenants about this purpose when you collected the information.

You may seek consent from tenants to allow you to do something that otherwise wouldn't be allowed under some of the privacy principles. If you believe on reasonable grounds that your tenants have authorised you to do so, you can:

- collect tenants' personal information from someone other than the tenants themselves (for example, from a credit reporting company or a referee)

- use or disclose tenants' personal information for a purpose other than the purpose for which you collected the information

Stating your purposes at the time of collection and asking tenants to agree to or acknowledge understanding of these purposes, can also be considered a form of consent.

When you're thinking about whether tenants have given informed consent to what happens with their information, try putting yourself in the shoes of an average person reading your forms and privacy statement. Would they clearly understand what you're planning to do with the personal information you collect, and are they able to say 'no' to things they don't feel comfortable with?

Here are some general principles to follow:

- Consent should be informed and specific. Tenants should clearly understand what they're being asked to agree to, and what will happen if they don't agree.
- You shouldn't bundle together multiple different things you want to do with tenants' information and ask them to agree to all of them at once. A tenant should be able to say which uses of information they agree to and which ones they opt out of.
- You shouldn't ask for broad agreement to collect information from 'other sources' or use information for 'other purposes.'
- You can't ask tenants to 'waive their rights' under the Privacy Act. This will have no legal effect.
- It's a good idea to allow tenants to change their minds and opt out of uses or disclosures they previously agreed to, if these uses or disclosures aren't related to your core purpose of managing the rental property.
- You can get consent verbally, but if you do it's a good idea to immediately record the consent in writing.

Tenant 'blacklists'

Landlords sometimes share information about tenants on so-called tenant 'blacklists'. These blacklists can be formal (such as a database held by a third party)

or informal such as a list hosted on a private social media group that's accessible only to group members. Using information supplied by landlords or other sources they claim to provide information about 'bad tenants' so that landlords can avoid renting to these tenants.

Tenant 'blacklists' are problematic under the Privacy Act. They lack transparency and are likely to contain information that's inaccurate or incomplete. They can unfairly keep tenants out of the rental market based on inaccurate information. They also represent a risk to the security of tenant information, as such lists could be leaked to unauthorised individuals. For these reasons, the use of tenant 'blacklists' has been criticised by groups representing both tenants and landlords.

If you submit information to such lists, you may be in breach of privacy principles 8 (accuracy) and 11 (disclosure). If you obtain information about tenants from 'blacklists' you may be in breach of principle 2 (collection directly from the individual), and if you use information from 'blacklists' without verifying its accuracy, you may be in breach of principle 8. If you manage such a list, you also risk breaching several privacy principles, and you should bear in mind that you must provide tenants with information you hold about them if they ask for it.

In addition, tenant 'blacklists' could breach other legal restrictions. The information on them could be defamatory. It could also breach suppression orders, including name suppression orders relating to Tenancy Tribunal proceedings that can be made under the Residential Tenancies Act.

Family violence

When selecting tenants, you shouldn't ask them whether they have experienced or are currently experiencing family violence. Such information is not relevant to deciding whether a person will be a suitable tenant and is highly sensitive. Asking potential tenants about family violence would be unreasonably intrusive.

If a current tenant tells you they are experiencing family violence, you should be particularly careful not to use or disclose that information unless you have reasonable grounds to believe the use or disclosure is allowed under one of the exceptions to the privacy principles. For example, you can disclose the information with the tenant's consent.

If you have good reason to believe a tenant is experiencing family violence, and that disclosure of their information is necessary to prevent a serious threat to the tenant's health or safety, or the health or safety of others, you can disclose information to the appropriate authorities.

Family Violence Withdrawal Notices

The Residential Tenancies Act allows a tenant to end a tenancy quickly to seek safety from family violence. You can read more on Tenancy Services website.

Key things to consider when handling sensitive personal information for a family withdrawal notice:

- do not ask for more information than required by the approved tenancy services form
- disclosure of a tenant's notice of withdrawal and supporting evidence is restricted by the Residential Tenancies Act (section 56E). You may only share this information if you have consent from the tenant, you are seeking legal advice or commencing legal proceedings, or if another relevant authorisation applies.
- Generally, this information should only be used for the purpose of allowing the tenant to end that tenancy
- When you no longer have a lawful purpose to retain the information you must securely dispose of the withdrawal notice and accompanying evidence. You cannot keep a record of the family violence withdrawal notice against the tenant's name if there's no lawful reason to do so.

OPC's approach to compliance with guidance

This guidance document outlines the Privacy Commissioner's expectations for handling personal information as a landlord and property manager. You can expect the OPC to respond to complaints, breaches, or non-compliance in line with this guidance. This is in line with our Compliance and Regulatory Action Framework.

The Privacy Commissioner may also proactively investigate privacy breaches and systemic privacy problems. The Commissioner can direct you to take action to comply with the Privacy Act

For more information

We have a large number of tenancy-related answers to common questions available on our AskUs database.

This guidance can't cover all the Privacy Act issues that might come up between landlords and tenants. More information is available on the Office of the Privacy Commissioner website www.privacy.org.nz or by emailing enquiries@privacy.org.nz or by calling 0800 803 909.

We strongly encourage landlords to learn more about the Privacy Act by doing our e-learning modules. You might also like to get expert advice from a lawyer or another privacy professional.