What to do if you think your privacy has been breached

If your complaint is

- about your personal information, and
- against a NSW government agency or local council,

you should normally seek an Internal Review. An Internal Review is an internal investigation that the government agency is required to conduct when you make a privacy complaint.

Other types of privacy complaints, such as complaints about your physical privacy, can be made to Privacy NSW.

For more information about your options, see the Privacy NSW brochure on *Making a Privacy Complaint*.

Where else you can go

The Office of the Federal Privacy Commissioner deals with complaints about Federal government departments and some parts of the private sector, such as health service providers and large businesses. For more information, phone 1300 363 992 or see www.privacy.gov.au

Privacy complaints about individuals such as neighbourhood disputes are usually best dealt with by mediation at a Community Justice Centre. See the White Pages for your local Centre or check their website at http://www.lawlink.nsw.gov.au/cjc

To find out more

If you would like more information relating to this brochure, NSW privacy laws or other privacy issues, please contact Privacy NSW.

Privacy NSW

web site: www.lawlink.nsw.gov.au/privacynsw
email: privacy_nsw@agd.nsw.gov.au

phone: (02) 9228 8585
fax: (02) 9228 8577

mail: GPO Box 6
Sydney NSW 2001

office: Goodsell Building, 8-12 Chifley Square
Sydney NSW 2000

privacynsw

Privacy NSW
Office of the NSW Privacy Commissioner

privacy nsw

Your Privacy

Protecting Privacy in NSW

privacynsw

What is Privacy NSW?

Privacy NSW is the Office of the NSW Privacy Commissioner.

Privacy NSW aims to protect and promote privacy in NSW. It assists government organisations understand and implement their privacy obligations and informs the people of NSW about what privacy means in their day-to-day lives.

The *Privacy and Personal Information Protection Act 1998*

The *Privacy and Personal Information Protection Act* (PPIP Act) explains how NSW State and local government agencies should manage personal information.

The PPIP Act offers the people of NSW enforceable privacy rights. It gives you the opportunity to make a complaint about a public sector agency if you feel it has misused your personal information.

What do 'Privacy' and 'Personal Information' mean?

There is no simple definition of privacy. It can mean the right to a sense of personal freedom, the right to have information about oneself used fairly, and a 'right to be left alone'. Many people confuse privacy with secrecy or confidentiality, but privacy is broader than both of these.

The fair use of 'personal information' is just one aspect of this broader concept of 'privacy'.

Personal information is any information or opinion about an identifiable person. This includes records containing your name, address, sex, etc., or physical information like fingerprints, body samples or your DNA.

The 12 Rules of Personal Information Protection

The Information Protection Principles (IPPs) are the backbone of the Act, and all NSW government agencies must adhere to them unless they have a lawful exemption.

They are summarised here:

Collection

1. **Lawful** – when an agency collects your personal information, the information must be collected for a lawful purpose. It must also be directly related to the agency's activities and necessary for that purpose.
2. **Direct** – your information must be collected directly from you, unless you have given your consent otherwise. Parents and guardians can give consent for minors.
3. **Open** – you must be informed that the information is being collected, why it is being collected and who will be storing and using it. The agency should also tell you how you can see and correct this information.
4. **Relevant** – the agency must ensure that the information is relevant, accurate, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

Storage

5. **Secure** – your information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.

Access

6. **Transparent** – the agency must provide you with enough details about what personal information they are storing, why they are storing it and what rights you have to access it.
7. **Accessible** – the agency must allow you to access your personal information without unreasonable delay and expense.
8. **Correct** – the agency must allow you to update, correct or amend your personal information where necessary.

Use

9. **Accurate** – agencies must make sure that your information is accurate before using it.
10. **Limited** – agencies can only use your information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which you have given your consent. It can also be used in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

11. **Restricted** – the agency can only disclose your information with your consent or if you were told at the time they collected it from you that they would do so, or if it is for a related purpose and they don't think that you would object. Your information can also be used without your consent in order to deal with a serious and imminent threat to any person's health or safety.
12. **Safeguarded** – the agency can only disclose your sensitive personal information without your consent in order to deal with a serious and imminent threat to any person's health or safety. Sensitive information may be about your ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.