

Where to get more information

Privacy / FOI Contact Officer
Legal Services
Central Support Office
Department of Juvenile Justice
Level 22
Sydney Central
477 Pitt Street
Haymarket NSW
PO Box K399
Haymarket 1240
Ph 02 9219 9442
Fax 02 9219 9414
www.djj.nsw.gov.au

Privacy Commissioner
Privacy NSW
Goodsell Building
8-12 Chifley Square
Sydney NSW 2000GPO Box 6
Sydney NSW 2001
Ph: (02) 9228 8585
Fax: (02) 9228 8577
Privacy_NSW@agd.nsw.gov.au
www.lawlink.nsw.gov.au/pc

Administrative Decisions Tribunal
Level 15, St James Centre
111 Elizabeth Street
Sydney 2000
Ph 02 9223 4677
Fax 02 9233 3283
www.lawlink.nsw.gov.au

Language assistance
Telephone Interpreting Service
Ph 13 14 50

Privacy Protection

Information for staff



PROTECTION OF PERSONAL INFORMATION

The *Privacy and Personal Information Protection Act 1998* (NSW) (the "PIIP Act") came into force on 1 July 2000.

Penalties are imposed by the Act that may be given if a public sector official deliberately discloses or offers to give out personal information outside of their lawful powers.

This Privacy Policy has been issued to inform clients, members of the public and staff of their rights and obligations under the PIIP Act.

What is Personal information?

The PIIP Act defines personal information as ..."information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can be ascertained from the information or opinion".

What is NOT personal information?

The PIIP Act excludes certain types of information from the definition of *personal information*. The most significant exceptions are information contained in a publicly available publication; information about an individual's suitability for public sector employment; information about a witness who is included in a witness protection program under the *Witness Protection Act 1995*; information about an individual that is contained in a protected disclosure within the meaning of the *Protected Disclosures Act 1994* (NSW),

THE INFORMATION PROTECTION PRINCIPLES

Information protection principle 1:

Personal information must only be collected for lawful purposes directly related to the function or activity of the department and where collection is necessary for that purpose.

Information protection principle 2:

Personal information must be collected from the individual to whom the information relates, unless otherwise authorised or the information is collected under an applicable exception.

Alteration of Personal Information

If someone believes the department holds incorrect or out-of-date personal information, they may seek to have their personal records amended under section 15 of the PIIP Act. A Juvenile Justice Officer or Admissions Officer may update a simple record of fact, such as address or phone number. For more complex matters, a written application must be lodged with the Privacy Contact Officer.

Complaints to the Privacy Commissioner

If a member of the public or an employee believes their privacy has been or might be breached in the future by the Department of Juvenile Justice, they can make a written complaint to the Privacy Commissioner who will investigate it and report to them.

The aggrieved person can also complain directly to the department.

Internal Review under Part 5 of the Act

The Department of Juvenile Justice can conduct internal reviews in relation to alleged breaches of the PIIP Act that occurred from 1 July 2000, which is the date of commencement of Part 5 of the PIIP Act.

All complaints, enquiries about information privacy, and requests for review should be treated as serious matters. If the direct-line manager is unable to assist, the complaint, enquiry or request should be directed to the Privacy Contact Officer, Central Support Office.

Individuals who have made an application for internal review may apply to the Administrative Decisions Tribunal (ADT) if they are not satisfied with either the findings of the review, or the action taken by the department in relation to their application for review. The ADT can make orders, including the imposition of fines up to \$40,000.

INFORMATION AND COMPLAINTS

Information about Personal information held by the department

People may apply under section 13 of the PIPP Act for information on:

- whether we hold personal information about them,
- if so, the nature of that information, and
- the main purpose for which the information is held.

To seek this information a person should contact the nearest Regional Office.

The department will endeavour to deliver this service without charge, however in some circumstances we may require a fee to cover expenses if extensive research is required.

In most cases an oral report to the person on the *nature* of the personal information held should suffice. For example, a person may be told that:

- personal information about the applicant is held on CIDS, and
- the information consists of identification details such as address, age, occupation and contact details.

A written response should only be required in complex matters, or if specifically sought by the applicant.

Access to personal information

People may apply for access to their personal information under section 14 of the PPIP Act. Access will comprise an inspection of documents containing the personal information unless information is stored in another format, such as on videotape. A client should not be given access to other documents that may concern them but do not contain personal information. These documents should be accessed under the *Freedom of Information Act 1989*. To arrange access, clients should contact the Privacy Contact Officer. We may charge a fee for access where it appears that the information requested could be sought under the *Freedom of Information Act 1989* or in such other circumstances we consider reasonable to do so to cover disbursements and expenses. Rates will be commensurate to those rates charged under the *Freedom of Information Act 1989*. Clients should be required to pay the fee before processing is undertaken.

Information protection principle 3:

Personal information must be collected in circumstances where the individual from whom it is collected is made aware of the fact that it is being collected, the purpose for collecting it, intended recipients of the information, whether the supply is mandatory or voluntary, relevant rights to access and correct the information and the name and address of the collecting agency and any holding agency.

Information protection principle 4:

Personal information must be collected taking reasonable steps to ensure the information is relevant, accurate not excessive and up to date and that the collection does not unreasonably intrude on the individual's personal affairs.

Information protection principle 5:

Where agencies store personal information they must ensure that it is kept no longer than necessary and disposed of appropriately, is protected by reasonable security safeguards, and protected from unauthorised use or disclosure when made available to a third party for a provision of a service to the agency.

Information protection principle 6:

Where the department stores personal information it must provide individuals with sufficient information about its holdings of personal information to enable the individual to exercise relevant rights.

Information protection principle 7:

This principle allows people a right of access to their personal information, which may be held by public sector agencies.

Information protection principle 8:

Where agencies store personal information they must comply with individual requests to amend their personal information to ensure that it is relevant up to date, complete and not misleading.

The PPIP Act sets up an alternative method of amending personal information held by public sector agencies to that which operates under the Freedom of Information Act 1989. Government agencies are

entitled to rely on any conditions or limitations imposed (on access or other matters) under the Freedom of Information Act.

Information protection principle 9:

Agencies proposing to use or disclose personal information must take reasonable steps to ensure its accuracy before use.

Information protection principle 10:

Agencies proposing to use or disclose personal information must use it only for the purpose for which it was collected, for a directly related purpose, for a purpose to which the individual has consented, where the use is necessary to prevent or lessen a threat to life or health or subject to an applicable exception.

Information protection principle 11:

If staff members propose to use or disclose personal information, they must only disclose it for a purpose directly related to a purpose of collection and where the individual is unlikely to object, where the individual has been put on notice that information is usually disclosed to the relevant person or body, where the disclosure is necessary to prevent or lessen a threat to life or health, or subject to an applicable exception.

Information protection principle 12:

Agencies proposing to use or disclose personal information must not disclose personal information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership unless disclosure is necessary to prevent or lessen a threat to life or health or is subject to an applicable exception.

WHERE DISCLOSURE OF PERSONAL INFORMATION IS AUTHORISED

Personal Information must only be disclosed with lawful authority

Before releasing private information that is held by the department, it is strongly advised that staff confirm that they are legally entitled to do so. Examples of lawful disclosure are when the information is required

- in connection with Court proceedings for an offence,

- for law enforcement purposes,
- in connection with a Youth Justice Conference,
- if authorised by subpoena or search warrant, or
- where the individual expressly consents to the disclosure.

If unsure whether the disclosure is lawful, the staff member should request advice from their line manager. If still unsure, it is advisable to obtain written permission from the person to whom the information relates. Failure to do so could result in the department and/or the staff member being fined. It is an offence under the PPIP Act for public sector officials to corruptly disclose or use personal information.

Disclosures in emergency situations

Personal information may need to be disclosed without consent when compelling ethical or legal reasons prevail, for instance:

- to fulfil legal or statutory requirements (eg child protection) or
- to protect clients, other individuals or the public where the practitioner becomes aware that there is a risk to the client's safety or that of others.

Before taking action to disclose personal information without consent, the level of perceived risk should be carefully assessed, preferably in consultation with a manager. Clients should be notified when disclosure without consent is intended or has occurred, unless this is contradicted by issues of potential harm or by legal provisions.

Disclosures to the Department of Community Services

Under section 248 of the *Children and Young Persons (Care and Protection) Act 1998*, employees have a duty to furnish information relating to the safety, welfare and well being of children and young persons to the Department of Community Services. The PPIP Act does not operate to prevent information exchange relating to welfare of clients or other children or young people between Department of Juvenile Justice and Department of Community Services.