



POLICY TITLE:	<u>PRIVACY, DIGNITY AND CONFIDENTIALITY</u>
POLICY NUMBER:	A 5
SECTION:	Organisational Policies
DATE APPROVED:	April 2003
DATE OF LAST REVIEW:	February 2008
NEXT REVIEW DATE:	February 2010
DATE AMENDED:	February 2008

Policy

Xavier complies with *The Privacy Amendment Act 2000* and follows the standards stated within the National Privacy Principles for collection, security, disclosure etc.

Each family's right to dignity and privacy is recognised, respected and protected in relation to their personal activities when receiving support through Xavier's services.

Xavier only records and maintains family and child information that is relevant to effective service delivery. Confidentiality is observed by all staff of Xavier both within the organisation and outside of it by ensuring that information about any family or child is given only on a 'need to know' basis through the case management process.

Information concerning a child supported by Xavier can only be released upon written consent of the parent/guardian. Parents also have the right to withdraw a consent for release of information at any time.

Xavier takes reasonable steps to ensure that personal information is protected from misuse, loss, unauthorised access, modification or disclosure. Personal information will be destroyed if no longer needed as per current legislative requirements.

Each family is aware of the information maintained by the service and has the right to see any information which the service keeps in respect of their family and/or children with a disability.

G. Lynn Card
Chief Executive Officer

PRIVACY, DIGNITY AND CONFIDENTIALITY PROCEDURES

PURPOSE AND SCOPE

Each consumer's right to privacy, dignity and confidentiality in all aspects of his or her life is recognised and respected.

RESPONSIBILITY FOR IMPLEMENTING PROCEDURES

All Staff

Procedure

Information collected by Xavier is necessary for the provision of services to families and supports the principles contained in the *Privacy Amendment Act 2000*, summary attached.

1. Parents are made aware of this policy via Xavier's Family Information Booklet. This booklet is provided to new families commencing with Xavier and on a regular basis/when updated to existing families. New families sign their receipt of the family booklet and verbal discussion of the privacy and confidentiality policy, on the Assessment Information Checklist.
2. Parents are also required to regularly sight and sign records such as:
 - Referral information
 - Care plans
 - Case management plans
 - Consent forms
 - Specialist reports, etc.
3. The information contained in a consumer's file, is available only to the consumer and those staff involved in direct service provision. Xavier managers are responsible for conducting regular client file audits which includes ensuring case notes are written in a manner that reflects dignity and respect.
4. Prior to information being released by Xavier to another service, individual or agency, written permission must be obtained from the guardian of the child with a disability. Only specific information listed on the consent to release form may be released to those specified on the form. See attached Personal Details Consent Form.

5. Verbal consent may be obtained from a parent/guardian by a Keyworker, Therapist or Manager when verbal information is to be exchanged. Verbal consent authorised by signature on the Personal Details consent Form and noted and dated in case notes.
6. All staff, management and consumers of this service are made aware of, and would be expected to adhere to, the privacy and confidentiality requirements of the service.
7. Xavier stores consumer's personal information in secure and up to date facilities and on protected computer equipment. Access is given to staff on a need to know basis.
8. To access information held by Xavier, the parent / guardian would need to make a request in writing.
9. Personal information will be maintained until the client reaches the age of 21 years after which if no longer needed, all personal information will be destroyed.
10. The Former Clients Register will be audited each December by the Administrative Assistants North & South to identify past clients who turned 21 years of age in the preceding 12 months.
11. Their personal information will then be removed from the archived files and destroyed by shredding and the client's electronic file will be deleted. This action will be recorded on the Former Clients Register.

Summary

The Privacy Amendment (Private Sector) Act 2000

The *Privacy Amendment (Private Sector) Act 2000* amended the Commonwealth *Privacy Act 1988* ('the Privacy Act') to establish minimum privacy standards for the Australian private sector, including for all private sector organisations that both provide health services and hold health information. The legislation applied from 21 December 2001.

What type of information is protected?

The Privacy Act protects 'personal information' about individuals - that is, any information recorded about a person where their identity is known or could reasonably be worked out.

Personal information includes a person's name, address, Medicare number and any health information (including opinion) about the person. Sometimes, details about a person's medical history or other contextual information can identify them, even if no name is attached to the record. This is still 'personal information'.

The Privacy Act does not cover de-identified statistical data, where individuals cannot reasonably be re-identified.

'Health information' is a particular kind of 'personal information' and attracts additional privacy protection because of its greater sensitivity.

'Health information' includes information about a person's health, disability, use of health services, or other personal information collected from someone when delivering a health service.

The National Privacy Principles (NPPs)

Ten NPPs form the core of the private sector provisions of the Privacy Act. These principles set the minimum standards for privacy that organisations must meet.

The principles cover the whole information handling lifecycle – from the collection of health information, to its storage and maintenance, as well as its use and disclosure.

The principles, as they might apply in the health sector, are summarised below.

NPP 1 – Collection and NPP 10 – Sensitive Information

These principles apply to the collection of health information. In general, they require a health service provider to:

- ❑ collect only the information necessary to deliver the health service;
- ❑ collect lawfully, fairly and not intrusively; and
- ❑ obtain a person's consent to collect health information about them.

Providers also need to ensure that consumers are informed about why their health information is being collected, who is collecting it, how it will be used, to whom it may be given and that they can access it if they wish.

NPP 2 – Use and Disclosure

This principle sets out how providers can use and disclose health information.

'Use' refers to the handling of information *within* an organisation.

'Disclosure' is the transfer of information to a third party *outside* the organisation.

A health service provider may use or disclose health information:

- ❑ for the main reason it was collected (the primary purpose); or
- ❑ for directly-related secondary purposes, if the consumer would reasonably expect these; or
- ❑ if the consumer gives consent to the proposed use or disclosure; or
- ❑ if one of the other provisions under this principle applies.

The key is to make sure that there is alignment between the expectations of the health service provider and those of the consumer about what will be done with the health information.

NPP 3 – Data Quality

Health service providers are required to take reasonable steps to keep health information up-to-date, accurate and complete.

NPP 4 – Data Security

This principle requires that health service providers take reasonable steps to protect and secure health information from loss, misuse and unauthorised access. Information that is no longer needed should be destroyed.

As health information may be needed for future care of the individual or for public health reasons, the priority should be to secure the data properly.

NPP 5 – Openness

Health service providers need to be open about how they handle health information.

A provider must develop a document for consumers that clearly explains how their organisation handles health information. The document must be made available to anyone who asks for it.

NPP 6 – Access & Correction

Consumers have a general right of access to their own health records.

Access can only be denied in certain circumstances - for instance where access can pose a serious risk to a person's life or health.

Also, consumers can ask for information about them to be corrected, if it is inaccurate, incomplete or out-of-date. The provider will need to take reasonable steps to correct the information.

NPP 7 – Identifiers

There are restrictions on how Commonwealth government identifiers, such as the Medicare number or the Veterans Affairs number, can be adopted, used or disclosed.

At present, a health service provider is not permitted to adopt these identifiers for their own record keeping systems. These identifiers may only be used or disclosed for the reasons they were issued or if other provisions under this principle apply.

NPP 8 – Anonymity

Where lawful and practicable, consumers must be given the option to use health services without identifying themselves.

NPP 9 – Trans-border data flows

If health information needs to be transferred out of Australia, this may occur if laws (or a scheme) with similar privacy protection to these principles bind the recipient.

Otherwise, health information should only be transferred with the consumer's consent, or if other provisions under this principle apply.

Complaints

Complaints about alleged breaches of privacy can be made to the Federal Privacy Commissioner. The Commissioner can investigate, conciliate and, if necessary, make determinations about complaints. However, the Commissioner will not investigate, unless the complainant has first complained formally to the health service provider concerned.