

Policy No: 5.10	Policy Name: <b>Privacy and Confidentiality</b>
-----------------	---

Applies to:	Version: <a href="#">2</a>
Specific responsibility:	Date Approved:
	Review Date:

## 1. Purpose

[Service name] is committed to protecting the privacy and confidentiality of clients, staff, [Board / Management Committee] members, students, volunteers and stakeholders in the way information is collected, stored and used.

This policy provides guidance on [service name] legal obligations and ethical expectations in relation to privacy and confidentiality.

[Service name] holds two types of information which are covered by this policy: personal and organisational information.

## 2. Policy statement

[Service name] is committed to ensuring that information is used in an ethical and responsible manner. [\[Service name\] will use its best endeavours to ensure that it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and service personnel.](#)

[Service name] recognises the need to be consistent, cautious and thorough in the way that information about clients, stakeholders, staff, [Board / Management Committee] members, volunteers and students is recorded, stored and managed.

All individuals, including clients, stakeholders, staff, Board members, volunteers and students have legislated rights to privacy of personal information. In circumstances where the right to privacy may be over-ridden by other considerations (for example, child protection concerns), staff act in accordance with the relevant policy and/or legal framework.

All staff, [Board / Management Committee] members, volunteers and students are to have an appropriate level of understanding about how to meet the organisation's legal and ethical obligations to ensure privacy and confidentiality.

## 3. References

Health Records and Information Privacy Act 2002 (NSW)

Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998 (NSW)

Part 13A of the Crimes (Domestic and Family Violence) Act 2007 (NSW)

Privacy Act 1988 (Cth)

Privacy Regulation 2013 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

## 4. Definitions

**Privacy provisions** of the privacy Act 1988 govern the collection, protection and disclosure of personal information provided to [service name] by clients, Board members, staff, volunteers, students and stakeholders.

**Confidentiality** applies to the relationship of confidence. Confidentiality ensures that information is accessible only to those authorised to have access, and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature e.g. it is information that is not available in the public domain.

**Consent** means voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.

**Individual** means any person such as a client, staff member, Board member, volunteer, student, contractor or a member of the public.

**Organisational information** includes publicly available, and some confidential information about organisations. Organisational information is not covered in the Privacy Act 1988 but some organisational information may be deemed confidential.

**Personal information** means information or an opinion (including information or an opinion forming part of a database) about an individual. It may contain information such as names, addresses, bank account details and health conditions. The use of personal information is guided by the Privacy Act 1988 and the Privacy Regulation 2013.

The **public domain** in relation to confidentiality is “common knowledge” i.e. information that can be accessed by the general public.

## 5. Procedure

### Dealing with personal information

[Service name] ensures mechanisms are in place to demonstrate that decisions and actions relating to privacy and confidentiality comply with federal and state laws.

All staff, volunteers, student and [Board / Management Committee] members are made aware of this policy during orientation.

All staff are provided with ongoing support and information to assist them to establish and maintain privacy and confidentiality.

In dealing with personal information [Service name] will use their best endeavours to ensure privacy for clients, staff, [Board / Management Committee] members and volunteers when they are being interviewed or discussing matters of a personal or sensitive nature. [Service name] will take reasonable steps to protect all health information and personal information from misuse and loss and from unauthorised access, modification and disclosure.

The privacy of personal information is defined by legislation (Privacy Act 1988, Privacy Regulation 2013). At all times, [service name] acts in accordance with these legal requirements. [Service name] also strives to respect the confidentiality of other sensitive information. However, in the spirit of partnership, we share information with clients and other involved individuals and organisations (subject to consent), where it would be in the best interest of the client or other individual to do so.

## Collection of information

Personal information collected by [service name] is only for the purposes which are directly related to the functions and activities of the organisation. These purposes include:

- Enquiry about programs
- Engagement in case management and support
- Administrative activities, including human resource management
- Sector development activities
- Community development activities
- Fundraising
- Complaint handling
- [COVID-19 vaccination status as part of NSW Government contract requirements](#)

[Service name] provides information to clients on collecting health and personal information including:

- Purpose of collecting information
- How information will be used
- Who (if anyone) information will be transferred to and under what circumstances information will be transferred
- Limits to privacy of personal information
- How a client can access or amend their personal information
- How a client can make a complaint about the use of their personal information.

Staff, [\[Board / Management Committee\]](#) members and volunteers are advised about [\[Service name\]](#) requirements to monitor and collect information on COVID-19 vaccination status as part of NSW Government contracting arrangements. Information gathered will be limited to what is required to meet reporting and service management requirements.

## Use and disclosure

[Service name] only uses personal information for the purposes for which it was given, or for purposes which are directly related to one of the functions or activities of the organisation. It may be provided to government agencies, other organisations or individuals if:

- The individual has consented
- It is required or authorised by law
- [Service name] has reasonable grounds to suspect that an unlawful activity has been, or may be, engaged in
- It will prevent or lessen a serious and imminent threat to somebody's life or health
- The disclosure is reasonably necessary for the funding, management, planning, evaluation, training of employees of the service or persons working with the service, and reasonable steps are taken to de-identify the information.

Further information regarding the use and disclosure of service user information can be found in the Access to Records Policy.

## Data quality

[Service name] takes steps to ensure that the personal information collected is accurate, up to date and complete. These steps include maintaining and updating personal information when we are

advised by individuals that it has changed (and at other times as necessary), and checking that information provided by another person about an individual is correct.

### Data security

[Service name] takes steps to protect the personal information held against loss, unauthorised access, use, modification or disclosure and against other misuse. These steps include reasonable physical, technical and administrative security safeguards for electronic and hard copy paper records as identified below. [\[Service name\] manager will initiate discussion on a regular basis with their information technology provider to ensure that all relevant safeguards are best practice and implemented.](#)

Reasonable physical safeguards include:

- Locking filing cabinets and unattended storage areas
- Physically securing the areas in which the personal information is stored
- Not storing public information in public areas
- Positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public

Reasonable technical safeguards include:

- Using passwords to restrict computer access, and requiring regular changes of passwords
- Establishing different access levels so that not all staff can view all information
- Using electronic audit trails
- Installing virus protections and firewalls

### Access and correction

Individuals may request access to personal information held about them. Access will be provided unless there is a sound reason under the Privacy Act or other relevant law. Other situations in which access to information may be withheld include:

- There is a threat to the life or health of an individual
- Access to information creates an unreasonable impact on the privacy of others
- The request is clearly frivolous or vexatious or access to the information has been granted previously
- There are existing or anticipated legal dispute resolution proceedings
- The request for access is of a kind that has been made previously on the same grounds and refused
- Denial of access is required by legislation or law enforcement agencies.

[Service name] is required to respond to a request to access or amend information within 30 days of receiving the request.

Amendments may be made to personal information to ensure it is accurate, relevant, up-to-date, complete and not misleading, taking into account the purpose for which the information is collected and used. If the request to amend information does not meet these criteria, [service name] may refuse the request.

If the requested changes to personal information are not made, the individual may make a statement about the requested changes which will be attached to their record.

The Service Manager is responsible for responding to queries and requests for access / amendment to personal information.

### Collection, use and disclosure of confidential information

Other information held by [service name] may be regarded as confidential, pertaining either to an individual or an organisation. The most important factor to consider when determining whether information is confidential is whether the information can be accessed by the general public.

Staff members are to refer to the Service Manager before transferring or providing information to an external source if they are unsure if the information is sensitive or confidential to [service name] or its service users, staff and stakeholders.

### Organisational information

All staff, Board members, students and volunteers agree to adhere to the [service name] Code of Conduct when commencing employment, involvement or a placement. The Code of Conduct outlines the responsibilities to the organisation related to the use of information obtained through their employment / involvement / placement.

### Staff information

The Human Resource Management Policy details how [service name] handles staff records to manage privacy and confidentiality responsibilities, including the storage of and access to staff personnel files and the storage of unsuccessful position applicants' information.

### Stakeholder information

[Service name] works with a variety of stakeholders including private consultants. The organisation may collect confidential or sensitive information about its stakeholders as part of a working relationship. Staff at [service name] will not disclose information about its stakeholders that is not readily available in the public domain without stakeholder consent.

### Service user information

Detailed information regarding the collection, use and disclosure of client information can be found in the Client Records policy.

### Breach of privacy or confidentiality

If staff are dissatisfied with the conduct of a colleague with regards to privacy and confidentiality of information, the matter should be raised with the staff member's direct supervisor. If a service user of stakeholder is dissatisfied with the conduct of [service name] staff or [Board / Management Committee] member, a complaint should be raised as per the Feedback and Complaints Policy. Information on making a complaint will be made available to clients and stakeholders and will be found on the [service name] website.

## 6. Related documents

- Client Records Policy
- Feedback and Complaints Policy
- [Mandatory COVID-19 Vaccination Policy](#)

## 7. Review

Reviewing and approving this policy		
Frequency	Person responsible	Approval

[How often will this policy be reviewed]	[Position of person responsible for reviewing policy]	[position of person/group who approves this policy]
--	---	---

Policy review and version tracking			
Review	Date approved	Approved by	Next review date
1			
2			
3			