Reference number:	**PY-OH-05 Privacy Policy**
Document owner:	Director, Finance and Commercial Services
Document approval:	Chief Executive Officer
Date document approved:	26.03.2021
Next review date:	26.03.2024

Policy statement

Odyssey House NSW (OHNSW) is dedicated to protecting the privacy of all affiliations with the organisation. This includes, but is not limited to; employees, clients, and other stakeholders (as defined). This policy defines the responsibilities of all in managing and dealing with sensitive information. It provides guidance on how the organisation collects, uses, discloses and otherwise manages personal information and provides guidance on legal obligations and ethical expectations in relation to privacy and confidentiality.

OHNSW have adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The APPs govern the way in which we collect, use, disclose, store, secure and dispose of all Personal Information. A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at https://www.oaic.gov.au/privacy/australian-privacy-principles/.

Purpose and scope

This policy ensures that:

- Odyssey House NSW provides quality services in which information is collected, stored, used and disclosed in an appropriate manner complying with both legislative requirements and ethical obligations.
- All employees understand their privacy and confidentiality responsibilities in relation to personal and organisational information about Odyssey House NSW, its clients, employees and stakeholders. This understanding is demonstrated in all work practices.
- Data breaches are dealt with in accordance with the Notifiable Data Breach (NDB) Scheme

OHNSW holds various types of information which are covered by this policy:

- Organisational information: some of this may be publicly available (i.e., found on the website or research articles) while there are other, confidential forms of information not available for public disclosure.
- Personal information: information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.' This applies to employees or stakeholders, and client records, towards addresses, medical history and treatment plans (see Appendix A). All of which is considered confidential and sensitive in nature. This information is not available for public disclosure beyond that which is posted on the website (i.e., information located on the 'About Us' section of the website), unless

permission has been obtained from an individual to allow disclosure and the person understands the implications of such disclosure.

Principles

Odyssey House NSW and its affiliates are responsible for preserving confidentiality and privacy in relation to information handling and utilisation, for the protection of clients, staff and other stakeholders.

During its activities, OHNSW may collect and store private and/or confidential organisational or personal information about members, stakeholders and employees. OHNSW is committed to ensuring that this information is used ethically and in a manner towards achieving organisational strategy and objectives.

Personal information is defined in the Privacy Act (1988), Schedule 1 APPs, to include information about such things as:

- an individual's racial or ethnic origin, political opinions, sexual orientation, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record, sexual orientation or health information.

Sensitive information will be used only:

- For the primary purpose for which it was obtained,
- For a secondary purpose that is directly related to the primary purpose,
- With consent; or where required or authorised by law.

Employee responsibilities:

- Upon employment, every employee of OHNSW must acknowledge and sign the confidentiality agreement, in understanding their responsibilities to the use of information for organisational operations.
- Every employee is responsible for the appropriate handling of such information and to prevent unlawful disclosure.
- If any employee has access to this information or such any personal information belonging to another employee or a client of the employer, or organisational information, they must maintain the confidence of any confidential information that they have access to, or become aware of, during their employment, and must prevent its unauthorised disclosure or use by any other person.
- Every employee will ensure that there is no use of confidential information for any purposes other than for the relevant and related employer processes during and after employment.
- Every employee is subject to the terms as outlined by the OHNSW Code of Conduct.

Client responsibilities:

- Clients who engage in treatment, either in Community Services or Residential Rehabilitation settings are subject to maintaining the privacy of the content of therapy and group sessions, especially in relation to other clients undergoing treatment. Every client has

a right to engage in treatment therapies with the confidence that their disclosures will remain within the context of therapy (see Client Charter and Client Consent to Treatment)

All stakeholders:

- Other stakeholders who engage in reviewing information, participating in organisational activities and other such means in which they are exposed to any information that could be considered personal or confidential in nature have a responsibility to preserve the integrity of the organisation and any individual associated with the information.
- No form of information, personal or otherwise, is to be utilised outside of organisational context in contributing to the objectives of the organisation.

COVID-19 health screening information:

- This data is collected and stored for a period of time for the purposes of contact tracing in the case that a stakeholder who has attended site potentially transmits the COVID-19 virus to others.
- This data is kept and stored for a period of 28 days, in accordance with the *Privacy Act 1988*.

Definitions

APPs: Australian Privacy Principles. Please refer to: https://www.oaic.gov.au/privacy/australian-privacy-principles/

Employee / Personnel: Any person who is employed, hired, retained or contracted to OHNSW (whether directly or indirectly or through a labour hire organisation) to provide support or other services, including Board members, Committee members, contractors, volunteers and students.

Clients: a recipient of OHNSW services.

Stakeholder: includes visitors, donors, and families and/or carers of clients.

Outcomes

This protection and confidentiality applies to any and all information pertaining to OHNSW during engagement as a stakeholder during and even after termination of relationship with the organisation.

In the event that this policy is breached, this will require investigation by the Privacy Officer and may result in disciplinary actions taken against the individual responsible for the breach, including, but not limited to:

- Termination of employment (as an employee);
- Termination from the program (as a client);
- Termination of relationship or engagement (as any other stakeholder);
- Potential legal action.

This will be decided on a case-by-case basis and align to PY-OH-07 Disciplinary Policy, and potentially PY-OH-08 Termination Policy.

Delegations

Board of Directors	• Have a responsibility to comply with the *Privacy Act 1988*.
Chief Executive Officer	• To approve this policy prior publication. • To inform the Board of any significant breach of data, including occurrences with legal implications. • To endorse any investigation of a significant consequence, which will be led by the Privacy Officer.
Director, Finance and Commercial Services **(Additionally, the Privacy Officer)**	• To undertake the role of 'Privacy Officer', as outlined by the *Privacy Act 1988*. • To manage and communicate any relevant notifications of Privacy updates and/or infringements to the CEO. • To be the lead investigator in any suspected or reported breaches of this policy.

Director, Programs	• Responsible for overseeing the management of privacy issues:
	  ○ Obtaining personal information from anyone accessing or seeking to access programs; and
	  ○ The storage and handling of personal information.

Manager, People and Culture	• Responsible for managing storage, use and breaches of employee information, including personal information and information pending to any ongoing investigations or cases. • To advise any relevant stakeholder around the responsibilities they have under the Code of Conduct.
Managers	• Ensure that staff are informed and trained to understand this policy and its implications. • To be the first point of contact for any breach of data.
All Staff	• To understand and comply with this policy and all affiliated policies referred to. • To maintain the confidence of any confidential information that they have access to, or become aware of, during their employment, and must prevent its unauthorised disclosure or use by any other person. This includes any client information (clinical and non-clinical), peers, management and organisational information.

Policy implementation

Employees

During recruitment processes, each employee must acknowledge and sign off a 'Confidentiality Agreement' prior finalisation of induction, as well as read through and understand the Code of Conduct. A breach of this agreement will result in disciplinary actions, up to and including termination of employment. Dependent on the extent of the breach, legal action may be actioned.

These principles apply during the course of employment and continue after separation from the organisation.

These principles apply equally to unpaid volunteer staff.

Clients

Upon admissions into the client services, both Community and Residential Rehabilitation, clients must acknowledge and agree to the 'Confidentiality Agreement', found in the 'OHNSW Admissions Form Package'. This agreement, in summary, outlines:

- OHNSW's responsibilities in keeping patient information secure.
- The conditions under which information will be released to a third party (i.e., under subpoena).
- Use of de-identified data for governmental reporting.
- Use of personal information in treatment.
- The responsibility of each client to not disclose information of others as presented during group activities.
- A client may request a copy of personal information recorded by OHNSW by providing proof of identity.

Financial Information

Financial information of clients, such as credit card and bank details, are managed under the Finance policies and PY-RC-13 Client Information Policy. It is important to note that no credit card information of clients is stored; credit card may be used one-off for client admissions, but these are processed immediately with the client (or a financial supporter of the client, e.g., parent or partner). Bank details are kept on file, but are protected by multi-factor authentication processes. Medicare numbers are stored for Centrelink purposes and as a form of client identification.

Marketing and promotion

Any information used in communications both internal and external to the organisation (e.g. social media) are governed by the APPs and the various Communications policies of the organisation.

Contractual and compliance obligations

Obligation to breach confidentiality

There are circumstances in which OHNSW is obliged to disclose confidential information to external bodies. These circumstances include:

- Third parties where the relevant person consents to the use or disclosure; and
- Where required or authorised by the law:
    - Subpoenas issued by a Court.
    - Request for information under Chapter 16A of the Children and Young Persons (Care and Protection) Act 1998 or other similar requirements, as per the *Privacy Act 1988*.
    - Mandatory Reporting; i.e., in the case of suspected abuse or neglect.

Overseas recipients

OHNSW will never disclose information to overseas recipients, unless permission has been gained to disclose that information.

Suspected Data Breach

As a relevant organisation covered by the *Privacy Act (1988)* OHNSW is obliged to comply with the Notifiable Data Breach Scheme.

A data breach occurs when personal information OHNSW holds is lost or subject to unauthorised access or disclosure, for example when:

- A device with a client's personal information is lost or stolen.
- A database with personal information is hacked.
- Personal information is given to the wrong person.

Should an individual feel that there has been a data breach affecting their personal information, and they had not been notified, they should immediately contact OHNSW and under the Scheme, OHNSW is obliged to respond within 30 days. If the response does not occur within this period, or the response is perceived to be insufficient, the individual has a right to lodge a formal complaint through the Scheme.

Under the scheme an eligible breach occurs if:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds,
- this is likely to result in serious harm to one or more individuals, and
- the organisation or agency has not been able to prevent the likely risk of serious harm with remedial action.

Under the scheme, if OHNSW becomes aware or suspects an eligible data breach they must:

- Quickly assess the incident to determine the likelihood of serious harm.
- Should the breach or suspected breach meet the criteria of Notifiable Data Breach, OHNSW must inform the OIAC and any individuals involved within 3 days. See for more information: https://www.oaic.gov.au/privacy/australian-privacy-principles/
- See the PY-IT-02 Security policy, which includes privacy, subpoenas and data breach.

OHNSW is subject to the NSW Health Grant Agreement, Standard Conditions, I light of potential cyber attacks to sensitive and personal information.

Related or Supporting documents

PY-RC-13 Client Information Policy
PY-HR-06 Grievance Policy
PY-OH-07 Disciplinary Policy
PY-OH-08 Termination Policy
PY-IT-02 Security Policy
Confidentiality agreement
Code of Conduct
rediCASE Software License Agreement - RSLA
Communications policies (PY-FM-01 – PY-FM-05)

References / Legislation

Children and Young Persons (Care and Protection) Act 1998 No 157
The Privacy Act 1988 (Privacy Act)
NSW State Records Act 1998
Australian Charter of Healthcare Rights (2008)
Australian Privacy Principles for Data Breach Preparation and Response- OAIC (2019)
Health Records and Information Privacy Act 2002 (HRIP Act, NSW)