PRIVACY MANAGEMENT PLAN

Laurel House
SEXUAL ASSAULT SUPPORT
COUNSELLING • EDUCATION • ADVOCACY • CHANGE

FEBRUARY 2024

Privacy Management Plan

1. About this Privacy Management Plan

Laurel House takes the privacy of our clients, employees, Board members, contractors and volunteers seriously. This Privacy Management Plan acts as reference and guidance tool for how we manage and protect personal information.

This Plan has been developed in accordance with directions of the Office of the Australian Information Commissioner's (OAIC) and will ensure Laurel House's adherence to the Australian Privacy Principles (APPs) as outlined in the *Privacy Act 1998* (Cth.). The OAIC also requires an organisation's Privacy Management Plan to be an action plan, which guides the establishment, implementation and continual review of the privacy management processes. Additionally, as Laurel House is funded by the Tasmanian Government, the plan also references the Tasmanian *Personal Information Protection Act 2004*.

The purpose of this Privacy Management Plan is to:

- Engender the trust of clients, staff and Board members, volunteers and contractors;
- Promote openness and transparency within Laurel House;
- Demonstrate how Laurel House complies with the *Privacy Act 1988* and the *Personal Information Protection Act 2004 (Tas);*
- Provide staff and volunteers (including Board) with the necessary knowledge and skills to manage personal and sensitive information appropriately;
- Clarify to staff, volunteers and clients the Organisation's obligations to disclose personal information in protection of children or when required to by law;
- Ensure clients, staff and other stakeholders understand how to make a complaint, and how they can access and/or correct their personal information.

2. Privacy Management Legislation

Laurel House, as a 'health organisation', is required to comply with the 13 Australian Privacy Principles (APP) of the *Privacy Act 1988*. Additionally, as Laurel House is funded by the Tasmanian Government, we also reference and comply with the Personal Protection Act 2004, and its PIP Protection Principles.

The APP principles and the PIP principles guide how Laurel House collects, stores, uses, and discloses personal and sensitive information. These principles cover the full 'life-cycle' of information protection from collection to disposal and establish obligations about data security, rights of access to and amendment of your own information.

3. Who does this plan apply to?

The plan outlines how we manage the personal and sensitive information of all people who interact with Laurel House. This includes our clients, their families and other service providers, our members, or Laurel House People including our employees, volunteers, students, contractors and Board Members.

4. Key Responsibilities

Laurel House Board (Board) - The Board is responsible for setting the direction, organisational culture, and identifying and mitigating risks that may impact on the delivery of services to clients and the wellbeing of staff. This includes the adoption and review of Laurel House's Privacy Management Framework.

Chief Executive Officer (CEO) - The CEO is responsible for ensuring that Laurel House establishes and maintains systems and processes for privacy management in compliance with the Privacy Act and investigating potential breaches of privacy.

Managers – Senior Staff are responsible for:

- making staff aware of this Plan and providing guidance on how to apply it,
- ensuring staff are provided with access to privacy training,
- identifying privacy issues when implementing new systems, and
- assisting staff to manage privacy issues.

All Laurel House People staff, board members, volunteers and contractors – All Laurel House People are responsible for being compliant with the content and intent of this policy.

5. Collection of Information

Laurel House collects the minimum personal and sensitive information from clients and staff members that is necessary for us to provide services and manage employment.

5.1 Collection of Information from Clients

When delivering services to clients we may seek to collect and hold the following personal and sensitive information:

Personal Information	**Sensitive Information**
• name, gender, contact details and address • date and place of birth • details of children • emergency contact details • photographs or other audiovisual material	• ethnicity and cultural background • Aboriginal or Torres Strait Islander status • health information including medical reports and management plans • vaccination status • information about current legal orders

5.2 Additional Requirements in relation to the Collection of Personal and Sensitive Information about Children and Young People

We collect personal information about children and young people under the age of 18 in order to deliver programs and services. We collect personal information about children, and young people only with the written consent of a parent or guardian or another authorised person, unless the child is taken to be sufficiently mature and has the capacity to make a decision about his or her own involvement with Laurel House and the collection of their personal information (i.e. considered "Gillick Competent" or a "Mature Minor").

5.3a Collection of Information from Members

We may seek to collect and hold the following personal and sensitive information of our members provided by members on their membership forms

Personal Information	Sensitive Information
• name, gender, contact details and address	• ethnicity and cultural background • Aboriginal or Torres Strait Islander status • information about disability and access needs

5.3b Collection of Information from Employees, Students, Volunteers, Contractors or Board Members

We may seek to collect and hold the following personal and sensitive information of employees, students, volunteers, contractors or Board Members:

Personal Information	Sensitive Information
• name, gender, contact details and address • date and place of birth • details of children • emergency contact details • photographs • licence or permits • qualifications, certificates • internet protocol (IP) addresses – for employees working from home only • Tax File Number • Bank Account Details • Salary Sacrifice Details • Superannuation membership details • Professional Registration details • National Police and Working with Vulnerable People checks, • Candidate information submitted to Laurel House including resumes	• ethnicity and cultural background • Aboriginal or Torres Strait Islander identifier • information about disability and access needs • health information including medical reports and management plans • vaccination status • information about current legal orders • information about criminal record, convictions or other notifiable disclosures (e.g. bankruptcy) • trade union memberships or associations, or political associations • information about other affiliations that may be considered potential, perceived or actual conflicts of interest (including intend to join or have failed to join the National Redress Scheme • information about incidents in the workplace • documentation in relation employment including training and development, performance appraisals and development plans, exit interviews etc.

5.4 How we Collect Information

We collect personal information by fair and lawful means. Where possible information is collected directly from you with your consent at the time of your interaction with us. We collect your information via face-to-face, telephone, and through other electronic and paper correspondence.

As far as practical we collect information directly from the people who use our services or work for us however, in some instances, personal and sensitive information is received from third parties (e.g. referees, referral agencies, police, child safety).

6. Use of Personal Information

We collect, hold and use personal information only for the original purpose for which it was collected. We will discuss with clients and employees how we will use and disclose their personal information at the time of collection.

We may also use information collected for the following purposes set out below including:

- To comply with the requirements of funding bodies as part of a funding agreement with us;
- To operate fundraising and charitable activities in support of our objectives;
- To provide customer service functions including handling customer enquiries, complaints and feedback;
- To gather feedback from you and other individuals about the quality of our services so that we can continuously improve;
- To facilitate proper governance processes such as risk management, incident management, internal and external audits;
- To satisfy legal obligations, comply with applicable laws and meet requirements of bodies that regulate our operations; and
- To understand, through aggregated information, trends and patterns which we use for research and advocacy.

7. Disclosure to Third Parties

We will not disclose personal or sensitive information to others including other external organisations except:

- As required by funding agreements (only deidentified information will be disclosed),
- As required by the law,
- Where a client has consented to sharing information with other services in order to provide holistic care,
- Where a client, volunteer, or employee has consented to a referral to an external organisations,
- Where an organisation or entity is subcontracted or engaged by us to complete work on our behalf, or in undertaking quality assurance of our services,
- Where an organisation or entity is engaged for the electronic storage of information.

We take our legal and moral duty to keep children safe very seriously. Therefore, we may disclose the personal information we hold where Laurel House has a legal duty to do so in relation to the safety and well-being of children.

Laurel House aims to work transparently with clients and ordinarily any information shared or reported in relation to the client is discussed with them if it is safe to do so. Where the

information provided is used to communicate with a client, the client will be provided with the opportunity to decline receiving communication from the organisation.

8. Storage of Personal Information

Personal information may be stored in hard copy form or electronic form. Hard copy records are required to be held securely. We hold electronic records in databases with security safeguards. Some of those databases are government controlled while some are held by third party providers. We store all personal and sensitive information in our secure corporate systems and in accordance with the Tasmanian *Archives Act 1983* store historic records in a state government accredited and secure records archive establishment.

9. Retention of Personal Information

We will retain your personal information in accordance with applicable laws, requirements of any government, or other funding body's record-keeping requirements.

10. Accessing or Amending Information

People who are subject to Laurel House's Privacy Policy/Plan can ask Laurel House for access to and/or amendment of the personal information we hold about them. Applications or queries should be directed to the Chief Executive Officer. Access to information does not necessarily mean access to copies of documents and we reserve the right to consider what information we can provide that will address your request for information, and we will provide this with consideration to the potential impact on your safety and the safety of others.

11. Client Use of Pseudonym or Anonymity

Clients of Laurel House are able to request that they use our services under a pseudonym or to be anonymous, where it is lawful and practical.

12. Cyber Security

Laurel House recognises that safeguarding personal and sensitive information requires a particular focus on cybersecurity. As part of continuously improving our cybersecurity efforts Laurel House commits to annual cyberhealth checks with a suitably qualified organisation. These annual cyberhealth checks should assess Laurel House's information technology environments and assets against the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) or another similar framework, and should provide recommendations on how to improve the organsiation's cyber security maturity capability. The annual assessment should seek to identify the strategies that are currently used to support 5 key pillars of a successful and holistic cybersecutiy program:

12.1 Identify

The Identify Function is focused on developing Laurel House's understanding of managing cybersecurity risk, to systems, people, assets, data and capabilities. As part of this function Laurel House will keep up to date inventories of devices, software platforms and applications, and external information systems, will ensure compliance with legal and regulatory requirements regarding cybersecurity and privacy, and will leverage the organisation's governance and risk frameworks. In order to strengthen this area, Laurel House will map organisation communication and data flows and

develop more explicit policies for staff and volunteers regarding data storage and cybersecurity.

12.2 Protect

The Protect Function outlines appropriate safeguards that ensure the delivery of critical data infrastructure, and support the ability to limit or contain the impact of a potential cybersecurity event. As part of this function Laurel House will ensure that access to physical and online assets are limited to authorised users and managed with the assessed risk of unauthorised access. This will include effective management of identities and credentials, limiting access permissions and authorisations using the principles of least privilege and separation of duties, careful management of remote access, and multi-factor authentication is activated wherever possible. Additionally, as part of this function Laurel House will engage a specialist organisation to provide cybersecurity awareness training to all staff and volunteers in a way that is proportionate to their individual needs, roles and responsibilities.

12.3 Detect

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. Laurel House has engaged specialist cybersecurity support to support our capability to continuously monitor the organisation's information systems and assets, and to detect unusual activity and events.

12.4 Respond

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident that will help to contain the impact of an incident. Laurel House has an Incident Response Plan and has the support of a highly specialist cybersecurity insurance provider and other cybersecurity specialists to assist in the event of a cybersecurity event. With the assistance of these specialists, Laurel House is building further maturity in responding to the changing nature of cyberincidents.

12.5 Recover

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities that were impaired due to a cyberincident, and to support any clients, staff, volunteers and other stakeholders affected by a cyberincident. Recovery is a key component of Laurel House's Incident Response Plan and it recognises the importance of prioritising the safety and wellbeing of clients and others affected by cyberincidents. The approach taken to recovery will include a continuous quality improvement approach that draws upon lessons learned and information gathered through engaging cybersecurity experts and the perspectives of our clients, staff, volunteers and others to guide our approach.

13. Data Breaches

We will comply with the notification and other requirements of the Act where your personal information held by us has been inadvertently lost or disclosed or improperly accessed and that loss, disclosure or access may result in serious harm to you.

14. Privacy Complaint Process

Any person who feels aggrieved by Laurel House's handling of their personal information is encouraged to lodge a complaint directly to the Chief Executive Officer, who is also the Public Officer. This could include any conduct or action we have taken or not taken.

All privacy complaints should ideally be addressed in writing to the CEO/Public Officer on ceo@laurelhouse.org.au or PO Box 1062, Launceston TAS 7250. Alternatively, for those where writing would be a barrier, they can call the CEO on 0427 739 397 or 6334 2740. Laurel House will conduct an internal review and has 30 days to respond to your complaint.

Where this issue is with the handling of personal information by the Chief Executive Officer, the complaint should be lodged with the Board Chair on president@laurelhouse.org.au or PO Box 1062, Launceston TAS 7250. Alternatively, for those where writing would be a barrier that can call Laurel House on 6334 2740 and ask for the Board Chair to call them. As above, Laurel House will conduct an internal review and has 30 days to respond to your complaint.

Should a person who has lodged a privacy complaint with Laurel House remain dissatisfied with the outcome of their complaint the next step is to contact the Office of the Australian Information Commissioner (OAIC). Details of how to do this can be obtained from their website https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us/ or by calling the OAIC Enquiry Line 1300 363 992.

You may also contact our funders to lodge a complaint about how your personal information was handled.

In relation to our Counselling and After Hours services, you can contact the Tasmanian Government's Department of Premier and Cabinet, Community Partnerships and Priorities Division, Level 4/15 Murray Street, Hobart TAS 7000GPO Box 65, Hobart Tas 7001 or email grants@dpac.tas.gov.au

In relation to our Disability Workforce project, you can make a complaint to the Australian Government's Department of Social Services at DSS Feedback, GPO Box 9820, Canberra ACT, 2601, or email complaints@dss.gov.au or via their Online Complaints Form

15. Privacy Impact Assessment

Laurel House will utilise a Privacy Impact Assessment (PIA) tool as part of its overarching Risk Management Framework to assess any actual or potential effects that an activity may have on personal information held by Laurel House.

16. Laurel House's Privacy Management Plan - Plan of Action

The OAIC outlines a four-step framework for meeting ongoing privacy compliance obligations (see image to right). As part of its Privacy Management Plan Laurel House has identified the specific, measurable goals and targets of how we will implement each of the four steps in the framework. The specific actions related to each of these four steps is outlined in an action plan that is for internal use only.