Title:	Privacy and Confidentiality Policy
Document type	**POLICY**
Document category	Governance and Risk
Mandatory for all staff	Yes
Date approved	02/08/2023
Review date	03/02/2029
Approval authority	Board
Contact Officer	Chief Executive Officer
Audience	All Staff
Related Documents	Child Protection Policy Complaints Handling Policy Code of Conduct Policy Managing Participant Disclosures of Criminal Activity Procedure
Legislation	Privacy Act 1988 (Cth) Health Records and Information Privacy Act 2002 No 71 (NSW) Privacy and Personal Information Protection Act 1998 (PPIP Act)

Table of Contents

1. Purpose

Human Nature protects the privacy of individuals and organisations in accordance with Australian Privacy Principles as set out in the Privacy Act 1988 (Cth)[1] and other relevant legislation.
The policy sets out the organisation's approach to collecting and holding confidential, private and sensitive information.

2. Scope

The policy applies to participants, parents/carers, employees , Board members, students, volunteers, donors and other stakeholders.

Human Nature holds various types of information which are covered by this policy including:

- Personal information
- Organisational information
- Health information
- Financial and donor information

We collect personal and health information from adolescents and their parents/carers for the purpose of providing mental health support and related services. This information may include:

- Contact details
- Health history
- Mental health assessments
- Treatment plans
- Progress notes
- Risk assessments

[1] Australian Government, Privacy Act 1988, accessed on 22/12/2022

3. Definitions

Term	Definition
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	A voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement.
Health Information	In accordance with the Health Records and Information Privacy Act 2002 No 71 (NSW), health information is: (a) personal information that is information or an opinion about— (i) the physical or mental health or a disability (at any time) of an individual, or (ii) an individual's expressed wishes about the future provision of health services to him or her, or (iii) a health service provided, or to be provided, to an individual, or (b) other personal information collected to provide, or in providing, a health service, or (c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or (d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or (e) healthcare identifiers, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for

Term	Definition
	the purposes of this Act generally or for the purposes of specified provisions of this Act.
Individual	Any person such as service user (participant), member, Board member, volunteer, student, contractor or a member of the public.
Information privacy	The way in which governments or organisations handle personal information such as age, address or sexual preference.
Notifiable Data breach	When: • there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds, and • this is likely to result in serious harm to one or more individuals, and • the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.
Organisational information	Information about organisations that may be publicly or privately available. Organisational information is not covered in the Privacy Act (1988) but some organisational information may be deemed confidential.
Parent/Carer	The parent(s) or carer(s) of the young person accessing Human Nature's Services.
Participant	A young person accessing Human Nature's services.
Personal information	Information or an opinion (including information or an opinion forming part of a database) about an individual (Office of the Australian Information Commissioner, 2019). It may include information such as names, addresses, bank account details and health conditions. The use of personal information is guided by the Privacy Act (1988).
Privacy provisions	As set out in the Privacy Act 1988, privacy provisions govern the collection, protection and disclosure of personal information provided to Human Nature by participants and other stakeholders, Board members, staff, volunteers and students.

Term	Definition
Public domain	In relation to confidentiality this means *common knowledge*, i.e. information that can be accessed by the general public.
Sensitive personal information	Sensitive personal information includes information about ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. Sensitive information, including health information, attracts additional privacy protections compared to other types of personal information.
Staff	Includes Human Nature employees, volunteers, Board members, students and contractors.
Substantial or material change	Any modification that significantly alters how personal information is collected, used, shared, or protected, impacting individuals' privacy rights or expectations.
Third Parties	Organisations or individuals outside of Human Nature with whom participant information may be shared. This includes service providers, government agencies, research partners, and other entities that require access to data for authorised purposes, such as fulfilling contractual obligations, complying with legal requirements, or providing necessary services.

4. Responsibility

Role	Responsibility
CEO	Approving the policy , ensuring potential or actual data breaches are evaluated and Notifiable Data Breaches are reported as required. The CEO Informs the Board of changes to the policy as required under the Policy Development and Review Policy.
Executive team	Monitoring implementation of the policy and providing staff with orientation and training to ensure they understand the policy.
Head of Marketing and Engagement	Ensuring that the Privacy Policy is available and up to date on the website.

Role	Responsibility
Clinical Manager	Ensuring that notification is provided to participants, family and carers of any substantial or material changes to the Privacy Policy within *10 business days* of updates.
Staff	Understanding and adhering to this policy and for reporting breaches, or suspected breaches, to their direct manager or the CEO.

5. Application

5.1 Collection of personal information

When Human Nature collects personal information, the information must be collected for a lawful purpose and must be directly related to the organisation's activities, and be necessary for these purposes. Information must be collected directly from the individual, unless consent has been given to obtain it otherwise. Parents/carers can give consent for minors.

Staff are required to ensure that the information is relevant, accurate, up to date and not excessive. The collection should not unreasonably intrude into an individual's personal affairs.

5.2. Accuracy of personal information

Human Nature acknowledges that individuals have the right to request access to personal information held about them and accordingly allows the individual to access, update, correct or amend their personal information as necessary.

When collecting personal and sensitive information, staff must advise individuals about how to access or change their personal information or to make a complaint about the use of their personal information.

- Participants are provided with information about their rights to confidentiality verbally and through consent forms and the parent and participant welcome packs, which also outline their rights to access information concerning their records.
- Participants, staff and other stakeholders wishing to change or access their personal information, or wishing to make a complaint about use of that information , can do so by contacting CEO via:
    - phone on 0477 176 312

- email: office@humannature.org.au
- mail: 111 Tamar St, Ballina.

5.3 Use and disclosure of personal information

Human Nature collects personal information for a variety of reasons including, but not limited to:

- documenting health care information and service provision
- seeking consent (e.g. media consent or consent required before an individual can take part in a Human Nature project or activity)
- research and evaluation purposes to inform services, campaigns and projects
- personal information, including photographs, video, or audio recordings of participants, whether de-identified or identifiable, with identifiable images or recordings only collected, stored, or used where written consent has been obtained
- details of individuals who join Human Nature as an employee, Board member, Youth Advisory Group member, committee member, student placement or volunteer
- donor and stakeholder records.

Human Nature can only use or disclose an individual's information for the purpose for which it was collected, for a directly related purpose, for a purpose to which they have given consent, to fulfil statutory requirements (e.g. reporting a serious crime), or when record subpoenaed by a court of law. Staff are prohibited from accessing private records that do not directly relate to their work and must not disclose private information to any unauthorised persons.

For further information about the retention and storage of health information as it applies to private health service providers in NSW, visit the Information and Privacy Commission of NSW website.

5.4 Photography, video and images

Human Nature recognises that photographs, video, and other images of participants constitute personal information and, in some circumstances, sensitive information. Human Nature does not take, use, or share photographs or recordings of young people without explicit, informed, and written consent, obtained and managed in accordance with the Consent and Decision Making Policy.

Consent for photography or recording is specific to the purpose and context for which it is sought, may be withdrawn at any time, and withdrawal will be actioned promptly without impact on a participant's access to services.

All participant images and recordings are stored securely on authorised Human Nature systems and platforms and are subject to the same access controls, retention, and security requirements as other personal information. Staff must not store participant images or recordings on personal devices, private phones, or personal accounts, or share them outside approved organisational systems or purposes.

5.5 Storage of personal information

Human Nature ensures each individual's personal or sensitive information is stored securely and held only as long as is necessary.

- Employment or contractor records must be kept for a minimum of five years as directed by the Australian Tax Office.
- Sensitive Health Information
    - For participants who were over 18 when the Health Information was collected: records are required to be held for 7 years from the last date of service
    - For participants who were under 18 when the Health Information was collected: records are required to be held until the young person reaches 25 years of age.
    - Must be disposed of securely and in accordance with any legal requirements for retention and disposal. Human Nature must also keep a record noting the:
        - name of the individual whose health information has been deleted
        - period covered
        - date the health information was deleted or disposed of.
- Donor and supporter records and other databases should be reviewed at least annually and records retired when they are no longer needed or when they have been unused for a period of 5 years or more.
- Other information about individuals should only be kept as long as necessary.
    - If personal information is no longer needed then it should be destroyed and disposed of in a manner where it will be protected from unauthorised access, use or disclosure.

- As required under privacy laws, any records kept by Human Nature regarding a participant's personal and/or health information must be up to date, accurate, relevant and complete, and not misleading.
- In the event of Human Nature's closure, arrangements will be made for secure record storage or transfer, with patient consent obtained for transfers.

5.6 Disclosure to Third Parties

The integrity of Participant's personal data is paramount. We restrict the release of Participant information to entities outside our organisation, except for specific, controlled circumstances. These include:

- **Contractual Obligations:** Disclosures mandated by funding agreements that underpin our service delivery.
- **Legal Imperatives:** Compliance with statutory requirements compelling information sharing.
- **Service Transition:** Facilitating seamless transitions to alternate service providers with Participant consent, as dictated by funding protocols.
- **Affirmative Consent:** When Participants (or their Families and Carers, through acceptance of this Policy, explicitly authorise disclosure related to the services we render.
- **Family and Carers:** Human Nature will not disclose personal information about Participants to parents/carers without their consent, except when the disclosure is required by law including concerns of risk of harm (see section 5.6)
- **Direct Requests:** Actions taken at the Participant's explicit direction (see section 5.6).
- **Insurer Requests**: Health information will only be released to insurers with the individual's explicit consent.

Examples of entities with whom information may be shared include:

- External service providers involved in Participant service transition.
- Government agencies, as mandated by funding agreements, potentially via direct database integration.
- Third-party service providers supporting service delivery, IT infrastructure, or quality assurance, potentially including overseas entities.
- Partners aiding in fundraising, donor analysis, and strategic development.
- Entities conducting research, service improvement, policy development, and advocacy through data analysis.

- Providers of electronic data storage solutions, which may be located internationally.

5.7 Sharing information with parents and carers of adolescent participants (aged 14-17)

Human Nature recognises the evolving capacity of adolescents to make decisions about their own lives, including their privacy. We prioritise the adolescent's well-being and safety in all decisions regarding information sharing, and maintain the confidentiality of information shared by adolescents, except where there is a legal obligation or a serious risk of harm. We are transparent about our information-sharing practices and provide clear explanations to adolescents and their parents/carers.

Human Nature may share information with parents/carers in the following circumstances:

- **With the adolescent's consent:**
    - We encourage adolescents to involve their parents/carers in their care where appropriate, and will seek their consent to share information.
    - We will discuss the benefits and risks of sharing information with the adolescent before seeking their consent.
    - We will document the adolescent's consent or refusal.
- **When required by law:**
    - We are legally obligated to share information in certain situations, such as when required by a court order or subpoena.
    - We are mandated reporters under child protection legislation and must report suspected child abuse or neglect.
- **When there is a serious risk of harm:**
    - We may share information without the adolescent's consent if we believe there is a serious risk of harm to the adolescent or another person.
    - This includes situations where the adolescent is at risk of self-harm, suicide, or violence.
    - We will make every attempt to discuss this with the adolescent before sharing, unless the immediate risk is too great.
- **For the purpose of providing care:**
    - Where sharing is necessary for the provision of care, and the adolescent is unable to give consent. This would be in situations of medical emergency, or unconsciousness, for example.

- **When the adolescent is under 16 and lacks capacity:**
    - When an adolescent under 16 lacks the capacity to make informed decisions about their care, we may share information with their parents/carers to ensure their best interests are protected.

Information we will not share:
We will not share information with parents/carers that:

- Is not relevant to the adolescent's care.
- Would breach the adolescent's confidentiality without a valid reason.
- Would put the adolescent at risk of harm.

5.8 Access to health information

5.8.1 Requests for access

Individuals may request access to their health information in writing, including their name, address, and specifying the information sought. Human Nature will respond within 45 calendar days, either granting access or providing a detailed reason for refusal, referencing the *Health Records and Information Privacy Act 2002 (NSW)*. Generally, adolescents aged 16 and over are presumed to have the capacity to make their own decisions regarding their health information and parents/carers typically do not have an automatic right to access their records without the adolescent's consent. For adolescents aged 14-15, capacity is assessed on a case-by-case basis. If the adolescent is deemed to have sufficient understanding and maturity to make decisions about their health information, their consent is required for parental access.

5.8.2 Refusal to access

Access may be refused if it poses a serious threat to health, impacts others' privacy, relates to legal proceedings, or for other reasons outlined in the *Health Records and Information Privacy Act 2002 (NSW)*. Any refusal will be accompanied by a clear explanation.

5.8.3 Fees for access

Human Nature may charge reasonable fees for providing access, covering costs such as administration and printing. Fees will not be excessive and will consider individual circumstances.

5.8.4 Deceased participant records

Requests for deceased patient records will be handled according to the Information and Privacy Commission NSW guidelines.

5.9 Data security

Human Nature 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 safeguards, including:

- Use of electronic databases and record storage protected by appropriately complex passwords and dual factor identification
- Establishing different staff access levels to information
- Implementing policies and procedures to safeguard personal information
- Training and orienting staff, Board members, volunteers and students about privacy and confidentiality
- Where cloud storage is used, Human Nature will take reasonable steps to ensure the cloud storage provider complies with applicable legislation and Australian standards including: Privacy and Personal Information Protection Act 1998 (PPIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act)
- Locking filing cabinets to securely store paper records and securing areas in which personal information is stored
- When working in public areas, positioning laptops so they cannot be seen/accessed by unauthorised people or members of the public.

In the event that a data breach occurs where personal information is accessed or disclosed without authorisation or is lost, Human Nature will immediately investigate the breach, and make notifications in accordance with the requirements of the Notifiable Data Breach (NDB) scheme.

5.10 Website privacy

Staff who are authorised to change content on the Human Nature website are required to recognise and consider privacy issues that may affect content including:

- personal information of staff presented to the public or other staff
- personal information of participants and members of the public included in web documents
- obtaining personal information from the public through their visit to the website.

Only those with authority under the Delegations Policy are permitted to make or approve changes to the website.

5.11 Social media

Content updated on social media sites, including but not limited to, Facebook, Twitter, Instagram, TikTok, LinkedIn and YouTube, must reflect this policy. Ways in which privacy can be protected through social media include:

- Privacy settings – all accounts have monitoring and privacy settings enabling authorised Human Nature staff to properly control the content that is posted on social media accounts
- Board members, staff and volunteers are prohibited from posting content on these platforms without consent or approval of the Head of Marketing and Engagement, the CEO or their delegate
- Media consent forms are required for the use of photographs or videos to promote Human Nature to donors and stakeholders, and on social media platforms, in accordance with section 5.4 of this policy and the section 6.6 of the Consent and Decision Making Policy.
- Staff must not add participants as their friends on their personal accounts
- Staff must have locked personal social media accounts so that participants cannot inadvertently add themselves to staff accounts.

5.12 Privacy policy maintenance

This Policy, along with the organisation's privacy practices, procedures, and systems, is periodically reviewed to ensure ongoing appropriateness in response to the evolving operational environment. Major updates will be communicated through regular organisational communications and by posting a revised version of this Policy on our websites, as outlined in Section 4 - Responsibility.

6. Policy breaches

All breaches of this policy will be taken seriously. Individual staff may face disciplinary consequences (including termination of employment for serious breaches), and the organisation may face legal action or fines if a breach of this policy occurs.

- Staff concerned about the conduct of a colleague with regards to privacy and confidentiality of information, should raise the matter with the staff member's direct supervisor or the CEO
- Information on making a complaint is made available to participants and parents/carers who can make a complaint in accordance with the Policy – Feedback and Complaints Handling.

7. Exceptions to this policy

There are legal limitations to confidentiality in the following circumstances:

- Where there is a serious and imminent threat to any person's health or safety
- In the reporting of a serious indictable offence as required by law (Refer Managing participant Disclosures of Criminal Activity Procedure).
- Where mandatory reporting of child protection concerns is required (Refer Child Protection Policy and Procedure).