PRIVACY POLICY

GPOL-010
Effective from 23 September 2024

1. PURPOSE AND SCOPE

The purpose of this document is to provide a framework for HWWC in dealing with privacy considerations.

HWWC is bound by the Privacy Act 1988 (Cth) and the privacy provisions of other applicable legislation and standards such as professional codes of conduct. HWWC must adhere to the Australian Privacy Principles in relation to collecting, holding, using, disclosing, securing, and allowing access to personal information.

2. POLICY STATEMENT

HWWC collects and uses a range of personal information for the purposes of providing health and support services to women and their families. The organisation is committed to protecting the privacy of the personal information it collects, holds and uses.

3. KEY DEFINITIONS

APPs	The Privacy Act 1988 (Cth) incorporates thirteen Australian Privacy Principles (APPs) that set out the rules for handling personal information
Personal information	Information or an opinion about an individual that directly or indirectly identifies a person
NDB	Notifiable Data Breaches

4. PROCEDURES

The personal information collected by Hedland Well Women's Centre (HWWC) may (but does not always) include:

- Clients: The names, contact information (e.g. mailing address, telephone number and email address), date of birth, gender and demographic details;
- Employees, students and volunteers (current and previous): names, contact information and employment history;
- National Police Checks and Working with Children Checks (Board Members, employees, volunteers and students including completed);
- The names and email addresses of persons who subscribe to the organisation's emails.

5. COLLECTION

The organisation aims to collect personal and sensitive information from the person themselves wherever possible. If collecting personal information from a third party, HWWC will advise the person whom the information concerns and from whom their personal information has been collected.

Sensitive information includes health information and information about race, gender, sexual orientation and other information.

6. WE COLLECT YOUR INFORMATION IN THE FOLLOWING WAYS

- During conversations with you, over the phone and/or face to face;
- Through your use of our website;
- From your referring doctor or any other persons/entities that have referred you;
- When you complete our forms and paperwork

We will collect personal and health information directly from you wherever reasonably practicable. However, sometimes we may obtain health information about you from your referring doctor, or any other persons/entities that have referred you.

Clients and employees are notified:

- about why the information is collected and how it is administered;
- That this information is accessible to them.

7. USE AND DISCLOSURE OF PERSONAL INFORMATION

HWWC only uses or discloses information for the primary purpose for which it was collected or for a directly related secondary purpose such as legal reasons or disclosure required to prevent serious or imminent threat to life, health or safety. For secondary purposes, HWWC will obtain consent from the affected person.

8. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

HWWC ensures that persons have access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up-to-date.

9. STORAGE, SECURITY AND RETENTION OF PERSONAL INFORMATION

HWWC understands the importance of protecting personal information from misuse, loss or unauthorised access or use and takes all reasonable steps to ensure that personal information is secure.

HWWC holds personal information securely through physical and electronic means. Hard copy files are stored in secure cabinets and employees are trained in privacy procedures. Security encrypted response forms are used to protect the personal and financial information provided over the Internet and secure online payment systems. IT systems are secured with firewalls and anti-virus scanners and information is stored in secure databases that only authorised employees have access to and only when required.

Board Members, employees, volunteers and students are required to sign a HWWC Confidentiality Agreement to ensure that issues of privacy are recognised and respected.

10. DESTRUCTION OF INFORMATION NO LONGER REQUIRED

- Any client information no longer lawfully required by HWWC is destroyed or de-identified unless the law requires otherwise;
- Personal information when not required is removed from decommissioned laptops and mobile phones;
- HWWC destroys records in accordance with the HWWC Policy and Procedure Manual for Client Records Management.

11. COMPLAINTS AND ENQUIRIES

Clients and employees should feel free to discuss any concerns, questions or complaints about any issues related to the privacy of personal information with the CEO or Management of HWWC.

If a person is dissatisfied, the HWWC Policy for Complaints should be followed. If not satisfied with how the matter has been handled by HWWC, the Office of the Australian Information Commissioner can be contacted via Privacy complaints | OAIC www.oaic.gov.au/privacy/privacy-complaints.

12. NOTIFIABLE DATA BREACHES SCHEME

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

A data breach involves the loss of unauthorised access to, or unauthorised disclosure of, personal information.

This Clause sets out the Response Plan to be undertaken by HWWC employees in the event that HWWC experiences a data breach or suspects that a data breach has occurred.

This Response Plan has been informed by the Office of the Australian Information Commissioner's 'Data Breach Preparation and Response' that can be found at https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response.

13. HWWC RESPONSE PLAN

13.1 ALERT

Where a privacy data breach is known to have occurred (or is suspected) any employee of HWWC who becomes aware of this must, within 24 hours, alert the CEO who will notify the Executive Chairperson.

Employees are required complete a 'HWWC Incident Form' for Privacy Data Breach to assist in documenting the required information.

13.2 ASSESS AND DETERMINE POTENTIAL IMPACT

Once notified of the privacy data breach, the CEO or Manager must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

Criteria for determining severity:

- The type and extent of personal information involved;
- Whether multiple individuals have been affected;
- Whether the information is protected by any security measures (password protection or encryption);
- The person or kinds of people who now have access;
- Whether there is (or could there be) a real risk of serious harm to the affected individuals (including physical, physiological, emotional, economic or financial harm);
- Whether there could be media or stakeholder attention as a result of the breach

or suspect breach.

The CEO or Manager must issue instructions as to whether the breach (or suspected breach) constitutes a Notifiable Data Breach (NDB) or whether the data breach should be managed at organisational level.

14. DATA BREACH CONSTITUTING AN NDB

The CEO or Manager must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

Notification to the OAIC should be made through the Notifiable Data Breach Form located at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

If practicable, HWWC must also notify everyone to whom the relevant personal information relates. Where impracticable, HWWC must take reasonable steps to publicise the statement (including publishing on the website).

15. DATA BREACH AT ORGANISATIONAL LEVEL

Where the CEO or Manager determines that the data breach is to be managed at organisational level, the CEO or Manager will evaluate the risks associated with the breach and ensure that immediate corrective action is taken to contain the breach, if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access or shutting down or isolating the affected system.

A report for submission to the Board and Management should be immediately prepared.

16. RESPONSIBILITIES

The CEO and Management are responsible for the implementation of this policy, for monitoring changes in Privacy legislation, and for advising on the need to review or revise this policy as and when the need arises.

The CEO and Management will ensure that stakeholders are aware of HWWC Policy for Privacy and its purposes and ensure this information is freely available in relevant publications and on the organisation's website.

17. AUTHORISATION

Certifies that the policy has been through all necessary procedures and is now in force.

- Full deliberation by the Board.

18. RELATED DOCUMENTS

Client Consent Medical Treatment Policy
Client Records Management Policy
Correct Client Identification Policy
Policy for Confidentiality
Policy for Feedback and Complaints
HWWC Clinic Operating Manual

19. REFERENCES

The Australian Privacy Principles