Womens Health & Family Services Policy for Privacy

1. Purpose

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

WHFS is bound by the Privacy Act 1988 (Cth) and the privacy provisions of other applicable legislation. In particular, WHFS must adhere to the Australian Privacy Principles in relation to collecting, holding, using, disclosing, securing and allowing access to personal information.

2. Principle

WHFS collects and administers a range of personal information for the purposes of providing health services to women and their families. WHFS acknowledges that information of a private and personal nature is obtained and aims to ensure that such information is respected as private.

Personal information is information or an opinion about an individual that directly or indirectly identifies a person.

WHFS recognises the importance of its stakeholders having personal information protected, administered securely and made accessible to them. The organisation is committed to protecting the privacy of personal information it collects, holds and administers. These privacy values are reflected in and supported by the organisation's core values and philosophies and also reflected in this Policy.

3. 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 WHFS Policy for Privacy and its purposes and ensure this information is freely available in relevant publications and on the organisation's website.

4. Australian Privacy Principles (APPs)

The Privacy Act 1988 (Cth) incorporates thirteen Australian Privacy Principles (APPs) that set out the rules for handling personal information. WHFS is committed to the implementation of the Australian Privacy Principles (APPs).

The Australian Privacy Principles are outlined at www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles. A copy of the Australian Privacy Principles is located on the WHFS Intranet.

5. Privacy Processes

The variety of personal information collected by WHFS may (but does not always) include:

- The names, contact information (e.g. mailing address, telephone number and email address), date of birth, gender and demographic details of clients.

- The names, contact information and employment history of employees, students and volunteers (current and previous). WHFS also collects and holds sensitive information of its Board Members, employees, volunteers and students including completed National Police Checks and Working with Children Checks.
- The names and email addresses of persons who subscribe to the organisation's emails.

6. Anonymity

WHFS permits clients from whom personal information is being collected to *not* identify themselves or use a pseudonym unless it is impracticable to deal with them on this basis.

7. Collection

The organisation aims to collect personal and sensitive information from the person themselves wherever possible. If collecting personal information from a third party, WHFS 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).

Clients and employees are notified

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

8. Use and Disclosure of Personal Information

WHFS 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, WHFS will obtain consent from the affected person.

9. Access to and Correction of Personal Information

WHFS 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.

10. Storage, Security and Retention of Personal Information

WHFS 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.

WHFS holds personal information securely through physical and electronic means. Physical access to offices is restricted. Hard copy files are stored in secure cabinets and storerooms 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.

WHFS establishes and confirms privacy compliance with providers of Information and Communication Technology services such as servers or cloud-based systems.

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

11. Destruction of Information No Longer Required

Any client information no longer lawfully required by WHFS is destroyed or de-identified unless the law requires otherwise.

Personal information when not required is removed from decommissioned laptops and mobile phones.

WHFS destroys records in accordance with the WHFS Policy and Procedure Manual for Client Records Management.

12. 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 WHFS.

If a person is dissatisfied, the WHFS Policy for Complaints should be followed using the Feedback and Complaints process as detailed on the WHFS website, contact page. If not satisfied with how the matter has been handled by WHFS, the Office of the Australian Information Commissioner can be contacted via www.oaic.gov.au/about-us/contact-us-page 'Privacy Complaints'.

13. 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 WHFS employees in the event that WHFS 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 'Guide to Developing a Data Breach Response Plan' that can be found at www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/guide-to-developing-a-data-breach-response-plan .

WHFS Response Plan

13.1 Alert

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

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

13.2 Assess and Determine Potential Impact

Once notified of the privacy data breach, the CEO or Executive 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 Executive 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.

13.3 Data Breach Constituting a NDB

The CEO or Executive 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, WHFS must also notify each individual to whom the relevant personal information relates. Where impracticable, WHFS must take reasonable steps to publicize the statement (including publishing on the website).

13.4 Data Breach at Organisational Level

Where the CEO or Executive Manager determines that the data breach is to be managed at organisational level, the CEO or Executive 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.