

## Privacy Policy

### 1. Purpose

Community Engagement (CE) is committed to protecting and upholding service users' privacy and dignity when dealing with personal information.

CE collects, stores and handles information in accordance with Inala Community House (ICH) Privacy and Confidentiality policies. Any information collected, is collected for the purpose of delivering responsive and relevant services to support service users. CE has strategies in place to protect personal information.

CE will ensure that consent is obtained by informing service users of the purpose of collection, use and disclosure. Service users will also be informed of when their information can be disclosed without consent.

ICH is committed to protecting personal information and upholding confidentiality, the ICH website has a Client Service Charter which outlines this and a separate Privacy Notice.

This policy must be read in conjunction with the ICH Privacy Policy. This policy outlines further requirements to protect privacy within CE.

### 2. Scope

This policy applies to all people working or engaged with Community Engagement (CE) and includes employees, volunteers, students, trainees, contractors and clients.

### 3. Policy

#### 3.1 Preventing Data Breaches

CE handles private information in accordance with the ICH Privacy Policy.

CE has strategies to prevent data breaches including:

- Physical files will be:
  - Kept locked when not in use and will never be accessible to service users or other visitors
  - Transported in lockable pouches
- Locking computers or other devices when not in use and not leaving this accessible to service users and other visitors
- Wi-Fi passwords will not be made available to unauthorised parties
- Information will be maintained in files until it is archived

### 3.2 Collection, Use and Disclosure

CE will:

- Provide information to service users about how their personal information will be handled through:
  - Client Service Charter will be displayed in all service delivery locations
  - Service User Rights and Responsibilities brochure will be available and displayed at all service delivery locations
  - Signs about cameras will be displayed at the entry to the service delivery locations
  - Privacy notices on all data collection forms (e.g. intake and assessment)
  - All service users will receive information about privacy
- Information is collected as relevant to the service user's goals, plans or in accordance with legal or funding requirements
- Ensure that records are accurate, up to date and complete
  - Case notes must be completed as soon as possible (preferably at the end of service user consultation) but no longer than 3 business days
- Not keep copies of credit or debit cards on file
- Collect information directly from service users except where consent has been provided to receive information from external parties. Consent may be collected in writing using the Authority Form or alternatively, information may be requested with the service user present and verifying their consent with the third party
- CE will only disclose information with the consent of the service user or in accordance with legal or funding requirements
- Respect an individual's request to remain anonymous or choice not to disclose their personal information. Where this occurs, workers will inform the individual of how this may impact service eligibility and delivery

### 3.3 Access Identification

CE workers must immediately report to the Manager when any breach or suspected breach of privacy occurs. The CE Manager will direct workers to take appropriate steps to remediate the breach or suspected breach and will report to the CEO.

### 3.4 Request for Information

Service users can access, correct and update their records by making a request to their normal worker or the Manager (CE). Service users can also withdraw or amend their consent.

Any service user or their authorised representative may make a request to access or correct their personal information in writing or verbally. CE will provide access or update personal information where requested except where an exception applies. Upon receiving a request, the worker must report the request to the Manager as soon as possible by close of business on the day of request. The Manager is responsible for approving any requests for information. Requests to access information may take up to five business days however it may take longer where information has been archived.

### 3.5 Responsibilities

Manager will:

- Review strategies to protect personal information and prevent unauthorised access, use or disclosure
- Ensure that workers are trained to uphold the privacy of service users and in accordance with the requirements of this policy
- Notify the CEO of any breaches or suspected breaches of privacy and take appropriate steps to remediate any breach
- Review any requests for access to personal information and ensuring that privacy and confidentiality obligations are upheld

Workers will:

- Take appropriate steps to safeguard the privacy of service user's personal information
- Report to the Manager any breaches or suspected breaches of privacy
- Report to the Manager any requests for access to service user's information

### 4. Review

This policy shall be reviewed every 3 years.

This policy remains in effect unless determined by resolution of the Board of Directors.

### 5. Related Documents

#### **Policies**

ICH Privacy Policy  
ICH Human Rights Policy  
ICH Service User Support Policy  
ICH Confidentiality Policy  
CE Service User Rights and Responsibilities Policy

#### **Legislation**

Privacy Act 1998  
Information Privacy Act 2009  
Right to Information Act 2009  
Human Rights Act 2019

#### **Other Documents**

ICH Service User Rights and Responsibilities Brochure  
ICH Client Service Charter  
ICH Privacy Notice