Privacy Policy

1. Purpose

Inala Community House collects and holds personal information for the purpose of carrying out services and in accordance with all legislative obligations. ICH will take all reasonable steps to protect and secure personal, sensitive, health and organisational information and to safeguard it from misuse or loss. Each service may have their own privacy requirements and if required will implement a policy to meet these requirements. ICH is also committed to ensuring any third-party providers of services (including cloud providers), are fully compliant with legislative and regulatory requirements.

2. Scope

This policy applies to all Board members, employees, contractors, students and volunteers. For the purpose of this policy, these persons shall be referred to as workers.

3. Definitions

Personal information: is defined in the Privacy Act 1998 as, 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not.'

Scope of personal information, as required by the *Information Privacy Act 2009* (Qld), applies to the:

- collection of personal information, regardless of when it came into existence,
- the storage and handling,
- accessing
- amendment,
- management, transfer, use or disclosure of personal information

This includes any information which means that an individual is reasonably identifiable.

Devices: includes any electronic device on which personal information is able to be stored. This may include handheld devices (e.g. mobile phones, tablets), as well as USBs, computers, hard-drives, etc…

Eligible Data Breach: is a notifiable breach which occurs where it meets the following criteria:

- There is unauthorised access or disclosure of personal information (or in circumstances where this is likely to occur)
- This is likely to result in serious harm to the individual

- Remedial action is not sufficient to prevent the likely risk of serious harm.

Serious harm: includes, but is not limited to psychological, emotional, physical, reputational, or other forms of harm.

4. Policy

ICH may require the collection of personal and sensitive information in order to carry out its services and in accordance with legislative or funding obligations. This may be collected and stored in a variety of ways including on devices, servers, cloud storage or paper files. ICH will take all reasonable steps to protect the privacy of individuals' information. This will be determined by considering the sensitivity of information, the possible harm resulting from a potential breach to an individual and to the organisation, and how the organisation stores or shares information.

4.1 Preventing Data Breaches

ICH recognises that the access to, or disclosure of personal information can result in serious harm for the individual including, but not limited to financial, emotional, physical or reputational loss or damage. ICH will take all reasonable steps to prevent misuse, interference, loss, unauthorised access, modification, or disclosure. Data breaches may occur through many avenues including IT resources, unauthorised access to information or breach of confidentiality. Management shall review and implement strategies to protect this personal information and shall train workers in the implementation of these strategies.

Strategies in place to protect and prevent these breaches include:

- Restricting access to personal information:
    - to those with a legitimate need to know
    - of those who no longer require access to that information (e.g. leaving the organisation or moving to another role)
- Limiting remote access to devices (except where authorised)
- Wi-fi network and cloud protection
- Access to electronic devices requires a PIN, password (using letters, numbers, punctuation or symbols, as appropriate) or encryption code
- File back-ups in case of system failure or natural disaster
- Regular updating of software to ensure that it is up to date
- Information which is no longer required to be kept shall be destroyed or de-identified (subject to other legal obligations)
- Physical files containing personal information are kept in a lockable storage area or transported in lockable pouches.
- Inspections of access permissions to ensure that these are appropriate and up to date when there are changes in personnel or at minimum on a quarterly basis
- Conducting a privacy impact assessment (as set out by the Office of the Australian Information Commissioner) for new programs, systems, databases, methods for collecting or handling information or changes in how information is stored

Information systems used by ICH will only store data on servers based within Australia. No information will be transferred outside of Australia unless authorised by the CEO in conjunction with any relevant funding body and where the person consents (or where s33 *Information Privacy Act* are met).

4.2 Collection, Use and Disclosure

ICH recognises that the collection of information, including personal, sensitive or health, enhances the organisation's ability to deliver core services. ICH will ensure that robust, accountable processes are developed regarding the collection of this information, ensuring that information sought and used is relevant to the services received and is appropriately managed. This includes:

- Ensuring that individuals are aware of the reasons for the collection of information and any law which authorises the collection, any parties to whom information is disclosed to (and if known, any parties that from that organisation further discloses to)
- Ensure that information collected is accurate, up-to-date and complete
- Advising how the information will be stored and used, in real time and backup
- Advising how information can be accessed, amended or corrected
- Obtaining individual consent for the collection of personal, sensitive or health information
- Data encryption, where appropriate, to further secure personal, sensitive or health information.

ICH does not keep copies of credit or debit cards on file.

ICH only collects information by lawful and fair means. ICH collects information in a number of different ways, and may hold information in either electronic and hard copy form, including but not limited to:

- Forms and plans (paper or online),
- Electronically, such as through ICH website contact forms or email,
- Phone calls and text messages,
- Information provided through service delivery interactions,
- Other correspondence, such as mail.

ICH will always collect personal information directly from the individual unless it is unreasonable or impractical for ICH to do so. On occasion, ICH may collect information from government, other involved services and professionals where an individual has expressly given permission.

ICH invests substantial resourcing into the establishment of secure information storage systems and will ensure that individuals are aware of how their information is stored.

ICH will support an individual's request to remain anonymous in the provision of personal information where it is reasonable and practicable to do so. ICH will advise individuals of the limitations to this prior to the collection of the information.

ICH will not disclose information without consent (including disclosure to subcontractors) except where required by law.

4.3 Access Identification

ICH will have strategies in place to identify unauthorised or irregular access to data. Systems are in place to eliminate access to data storage systems where an irregularity is detected. ICH systems are monitored in order to ensure the security of personal information.

If workers become aware of a breach or suspected breach, this should be reported to their Manager so that appropriate actions may be taken.

As soon as a suspected breach has occurred, ICH will take steps to contain the alleged breach of personal information. Remedial actions should seek to prevent further unauthorised access or disclosure of personal information. Examples of this may include:

- Wiping information on a device when the device is lost or stolen
- Contacting a person and asking them to delete an email where it has been accidentally addressed to the wrong person.

ICH complies with all requirements of the national Privacy Principles through taking reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under 'Use and Disclosure' Principle 6.

4.4 Assessment and Documentation

All suspected data breaches must be investigated by ICH. An assessment must consider:

- How the breach may have occurred
- Whether there are any vulnerabilities in the information security protocols or training. If so, what actions can be taken to prevent further breaches.
- Whether the breach is an 'eligible data breach'
- What type of harm may likely result from this breach

Assessment should be completed within 30 days of the suspected breach and conducted as expeditiously as possible so that further action can be determined which may minimise the breach or prevent a further breach occurring. All documentation and assessments of 'eligible data breaches' should be evidence-based. All suspected data breaches (whether actual or not) should be documented and forwarded to Human Resources and the CEO.

4.5 Notification

If an 'eligible data breach' occurs, then it is necessary to notify both the individuals to which the information relates and the Australian Information Commissioner. This must occur as soon as practicable once there is a reasonable belief that an eligible data breach has occurred. ICH may notify all individuals at risk of serious harm or where this is not practicable, publish a statement on the website and publicise it.

ICH will report any eligible data breaches to relevant funding bodies and other authorities in accordance with relevant legislation.

4.6 Complaints and appeals

Individuals will be made aware of their rights to report actual, suspected or perceived breaches of privacy and how they can make these complaints. These complaints can be lodged internally at a service level with the Manager. A privacy complaint will be responded to within 45 days. External complaints can be lodged with the Office of the Australian Information Commissioner or other statutory bodies.

If someone is dissatisfied with the outcome of a complaint, they may lodge a complaint with the Australian Information Commissioner via: https://www.oaic.gov.au/privacy/privacy-complaints/

4.7 Notifiable Data Breaches

The Privacy Amendment (Notifiable Data Breaches) Act 2017 established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the Australian *Privacy Act 1988* (Privacy Act) from 22 February 2018.

The NDB scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (OAIC) must also be notified of eligible data breaches.

4.8 Review

Using the findings from the assessment phase, ICH will review the incident and identify methods to improve the personal information privacy systems in order to prevent a further breach.

4.9 Request for Information

Individuals may make a request for access to or to correct their personal information. ICH will provide this information except where an exception applies. Authorisation for disclosure will involve several steps to ensure that ICH is compliant with privacy laws and any other requirements. When a request for access is received, the service to which the request relates must collate the information, withholding any information which cannot be disclosed. The Manager of that service should confirm this information complies with privacy or other requirements. Where information is released to a service user or their representative or in accordance with delivering the services, these disclosures shall be documented on the service user's file.

For services funded by a Queensland Government department, service users have the right to apply for access to, or amendment of information held by the department in accordance with the *Right to Information Act 2009.*

5. Review

This policy shall be reviewed every 3 years.

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

6. Related Documents

Policies

ICH Code of Conduct Policy
ICH Confidentiality Policy
ICH Conflict of Interest Policy
ICH Remote Work Policy

Form

ICH Consent to Disclose Information Form

References

Privacy Act 1998 (Cth) including obligations within Australian Privacy Principles (or APPs).
Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
Information Privacy Act 2009 (Qld)
Right to Information Act 2009 (Qld)
Competition and Consumer Act 2010 (Cth) in particular Schedule 2 Australian Consumer Law (ACL)
Family Law Act 1975 (Cth)
Australian Human Rights Commission Act 1986 (Cth)
Queensland's Human Rights Act 2019 (Qld)
In addition, any Queensland specific consumer law prior to 1 January 2011.