PRIVACY & CONFIDENTIALITY POLICY & PROCEDURES

Preamble

Kyabra respects that information shared by service users/employees belongs to those service users/employees. Kyabra aim's to uphold the highest standards of service users'/employees' rights to confidentiality and privacy by abiding by the Australian Privacy Principles, the relevant national and state legislation, and relevant funding body requirements.

Policy

Kyabra shall collect only such personal information from service users as is necessary to provide the service offered to or sought by them.

Service users/employees shall be given full disclosure of what information is to be held and how it may be used. The service user/employee will be offered the right to inspect any information held and to correct inaccuracies.

Information will be securely stored and accessed only by those employees whose job makes it necessary for them to do so. No information will be shared with a third party without the service users'/employees' permission, except where issues of personal risk or public safety make it legally or ethically mandatory that we do so. However, records may be used in statistical analyses so long as individuals cannot be identified.

Private records shall be destroyed or de-identified when not further required, except where legal requirements or public safety considerations make it necessary or prudent for us to retain them for longer.

Kyabra shall put in place procedures to ensure the privacy, safety and security of service users' /employees' information and to ensure that service users and employees are aware of their rights and responsibilities with regard to privacy matters.

This policy applies to anyone who engages with Kyabra services whether via Kyabra's website, email, phone, and/or videoconferencing platforms, or in person.

Ratified by Executive Board: 26th March 2018
Date of last review: August 2025
Date for next review: August 2027

Procedures

Collection

Potential service users will be made aware of Kyabra's confidentiality and access to information practices during initial visit (or initial phone call). Where possible, this information is to be given to service users verbally and in writing. All employees, and where possible, service users are to sign a *Rights and Confidentiality form*, which will then be kept on that individual's file.

During collection of information, it is important to explain why the information is being collected and to whom the information will be disclosed.

Use and Disclosure

Any information collected from service users will only be used for the purpose of providing the service offered to, or sought by, them.

Anonymity

An individual can contact Kyabra on an anonymous basis or using a pseudonym, however it may impact Kyabra's ability to provide information, supports and services to that individual.

Overseas Use or Disclosure

Generally, Kyabra will only transfer personal information overseas where the individual expressly consents to such transfer. However, given the amount of electronic contact information collected by Kyabra (and Lighthouse Resources) and that many software vendors and service providers are outside of Australian boundaries, information may be transferred outside of Australia in the course of managing that information. Before transferring any information outside of Australia, Kyabra will take reasonable steps to ensure that:

- The information belongs to people over the age of 18 years;
- Any service provider who will be handling the information will be contractually bound to comply with the *Privacy Act 1988 and Information Privacy Act 2009*; and
- The country to which the information is to be transferred has a system of Privacy protection at least equal to the Australian system and incorporates a means of taking action for any breaches of Privacy.

Countries to which information may currently be transferred for the purposes of management of personal information include:

- United States of America.
- Ireland (in relation to Bamboo HR software)

Data Quality

Kyabra workers will take all reasonable steps to ensure that information collected about an individual is accurate, complete and up-to-date at the time of collection and use.

Data Storage and Security

Kyabra will take all reasonable steps to ensure that data is kept safe from misuse, loss and/or unauthorised access. This includes:

- Using secure filing cabinets for hard copies and password-protected files for electronic data.
- Using appropriate firewalls and network protection software
- Only permitting authorised personnel to access personal and sensitive information.
- Ensuring personal and sensitive information is destroyed in a secure manner.
- Regular back-up systems are in place to save data from being lost

Information that is no longer required will be destroyed or de-identified, after seven years, except where legal requirements make it necessary for it to be retained for a longer period. Personnel records, incident and investigation reports, liability insurance policies and other relevant incident related correspondence shall be retained for a period of 50 years.

Database Access

Information pertaining to service users will, in most cases, be stored on Kyabra's Service Record System. Information pertaining to NDIS Participants who are accessing Kyabra's Support Worker Services will be stored on the MYP Platform. These electronic databases contain private and confidential information and only authorised staff* will be granted permission to access the databases. Each user is given a unique user name and password. All access to the SRS database is logged and is subject to regular audits.

*(*Staff roles that have permission to access the database are listed below under 'Access and Correction')*

Openness

A fact sheet on Rights, Privacy and Confidentiality will be given to service users at the commencement of service which includes how to access Kyabra's Privacy and Confidentiality Policy. Kyabra keeps an updated copy of this policy on the Kyabra website (*www.kyabra.org*).

Access and Correction

Service users and employees are able to access and check the information which is held by Kyabra as per the *Access/Amend Personal Information Policy and Procedures*.

The following positions within the organisation will be granted access to the service users' files section of the Service Record System (SRS) Database, pertaining to their geographical area of work, and relevance to their roles:

- CEO
- General Managers
- All managers and members of the following teams:
    - Intake & Assessment (including reception staff)
    - Case Management & Coordination
    - Group Work & Training (with the exception of Early Year's Workers)
    - Quality Assurance & Continuous Improvement
    - Organisational Services
    - Accommodation and Domestic & Family Violence Support Service
    - KEIHS (Keys to Early Intervention Homelessness Service)
    - Safe and Connected Housing Service

The following positions within the organisation will be granted access to the NDIS Participants' files section of the MYP Database:

- Support Worker Services – office-based staff
- Project Officer, Quality Assurance

Kyabra's IT Manager and IT staff will have access to the SRS database and MYP Platform for the purposes of setting up staff access and removing access for exiting staff, but will not have access to service user files.

Breaches of Privacy

Kyabra's *Complaints and Feedback Policy and Procedures* should be followed if any individual is concerned about a possible/actual breach of privacy. If an appropriate outcome is not achieved via this process then the Information Commissioner can be contacted. For more information refer to www.oic.qld.gov.au.

Kyabra has an obligation to report any breaches of privacy immediately to the relevant funding bodies. This includes any incidences of lost, damaged or compromised security of client personal information. Kyabra will also notify the client involved, relevant Manager, Organisational Management Team (OMT) and record any incidences on Kyabra's Risk Register.

Kyabra also has obligations under the 'Notifiable Data Breaches Scheme' to report any data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'.

Examples of a data breach include the following incidents:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

There are a few exceptions, which may mean notification is not required for certain eligible data breaches.

In the event of an 'eligible data breach' then Kyabra will follow the guidelines and procedures set out by the Office of the Australian Information Commissioner (OAIC). This includes notifying the OAIC of the data breach via their Notifiable Data Breach Form.

Definitions:

Personal Information is defined by the Privacy Act 1988 as any "i*nformation or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".*

Sensitive Information is a subset of personal information and is defined by the Privacy Act 1988 as:

- information or an opinion (that is also personal information) about an individual's:
    - racial or ethnic origin
    - political opinions
    - membership of a political association
    - religious beliefs or affiliations
    - philosophical beliefs
    - membership of a professional or trade association
    - membership of a trade union
    - sexual orientation or practices, or
    - criminal record
- health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates

Health Information is defined by the Privacy Act 1988 to mean:

- information or an opinion, that is also personal information, about:

    - the health or a disability (at any time) of an individual, or
    - an individual's expressed wishes about the future provision of health services to him or her, or
    - a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a health service, or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Relevant Legislation:

- *Information Privacy Act 2009 (Qld)*
- *Privacy Act 1988 (Commonwealth)*
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*
- *Domestic and Family Violence Protection Act 2012 (Part 5A)*
- *Human Rights Act 2019 (Qld)*

Relevant Documents:

- *Access/Amend Personal Information Policy and Procedures*
- *Rights and Confidentiality form/Permission to Share form - Community members*
- *Rights and Confidentiality form – Staff and Volunteers*
- *Application to View/Amend Kyabra File Form*
- *Guidelines around Notifiable Data Breach Scheme* - https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme