POLICY	PRIVACY AND CONFIDENTIALITY POLICY
Related Section	Governance

STATEMENT

We are committed to maintaining the privacy and confidentiality of participants, employees, others and the business functions associated with us.

PURPOSE

We aim to ensure our legal and ethical responsibilities are upheld in terms of the confidentiality and privacy of participants, employees, and any organisational information that is deemed to be private.

We protect and handle personal information in accordance with legislation and only collect, retain and use personal information in order to provide a safe working environment and a high standard of quality services. The information we collect is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

SCOPE

This policy applies to:

- all personal information and sensitive personal information including the personal information of employees and participants,
- all company confidential information - that is any information not publicly available,
- all representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

DEFINITIONS

Types of information and collection of information.

Personal information is any recorded opinion or information that identifies or could be used to identify an individual (e.g. name or date of birth), regardless of whether it is true. Personal information is only collected where the information is necessary for us to provide services and/ or undertake our business functions. The individual collecting the information must ensure that it is accurate, complete, and up to date. The purpose for collecting must be disclosed to the individual before, during or as soon as practicable after the collection of personal information from an individual (or from their authorised representative). The employee must take reasonable steps to make the individual aware of:

- Our organisation's identity and provide our contact details,
- Why the information is being collected,
- Any law that requires the information to be collected,
- The consequences, if any, if all or part of the information is not provided,
- Their right to access the information,
- Any third parties who may have, or be given, access to the information.

Sensitive information: Some personal information is also considered sensitive information and is therefore given special treatment. Health information is regarded as one of the most sensitive types of personal information and therefore, extra safeguards are in place when handling health related information. When collecting sensitive information, the individual must provide consent. Exceptions to the consent include where it is required:

- To prevent or lessen a serious and imminent threat to the life or health of an individual,
- Under legislation or is authorised by law,
- For the establishment or defence of a legal or equitable claim,
- For certain services where the sensitive information cannot be collected with consent.

Confidentiality

It is expected the Board of Directors and all employees will respect the confidentiality of information obtained during their role with Alkira and any meetings they attend. Information will not be shared, or any references, about employees, participants or business activities to networks outside of Alkira.

Alkira employees will also respect the confidentiality of information obtained during service delivery, networks and referral services.

Employees are expected to inform participants and/ or their representative about the *limits of confidentiality* in any given situation and inform people about the purposes for which information is obtained and how it will be collected, held, used, and disclosed.

At times, staff may be required to share information with management, including for the purposes of supervision and debriefing, and this information shall remain confidential except where it involves:

- Serious illegal actions on the part of participants,
- Issues which have the potential to endanger the safety of themselves, other participants, Alkira employees and/ or the wider community,
- the employee's obligation to make a mandatory notification to legal bodies and/or government departments, such as the Department of Health & Human Services, as defined by the relevant legislation or funding guidelines,
- Any other issue that employees are legally obliged to disclose.

This must be discussed with management to determine the most appropriate course of action prior to notification or reporting made.

There are at times, under legislation, where staff may be required to share information, without consent, regarding a participant or an employee. This is only done in compliance with relevant legislation processes and must be approved by the relevant management prior to release.

A data breach is type of security incident where personal, sensitive or confidential information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen or used by an unauthorised person or parties. A data breach where people are at risk of serious harm as a result, is reportable to the Office of the Australian Information Commissioner.

PRINCIPLES

Confidentiality can be assured by adhering to the following principles:

- Confidential information, participant files, faxes, emails, mail, and other printed matter must not be left out on desks, the photocopier, fax machine or other office equipment where a breach of confidentiality or privacy may occur,
- When sending confidential information, employees must ensure the recipient of such is aware of the confidential nature of the information contained therein and must ensure it is sent to the correct address,
- As relevant, passwords should be attached to "confidential" files,
- Employees will not disclose their passwords to any other employees,
- When working on or looking at a confidential document on your computer, employees shall ensure it is not exposed to others who are not authorised to view.
- Minutes, agendas, or notes of confidential meetings shall be filed away and kept in a secure environment,

- When discussing confidential information take appropriate measures to ensure your conversation cannot be overheard,
- All personal information is held under secure conditions with access restricted to those who need it to carry out their role and position,
- Participant information is kept on Alkira needs to know basis. Paper copies are stored in locked storage,
- Alkira ensures participant sensitive data is sent to government agencies under secure conditions. No data is sent overseas.

New employees starting with Alkira are expected to complete privacy and confidentiality training and/ or education and maintain knowledge and skills through any ongoing updates and changes.

Any information given to unauthorised personnel will result in disciplinary action. Alkira employees are bound by their position description, contract of employment and code of conduct to maintain privacy and confidentiality at all times.

If there is a breach of a person's information and their private/ confidential data is inappropriately shared, the person/s whose information has been released will be informed and communicated as per the "Notifiable Data Breach Scheme" and using the four key principles: - contain, assess, notify & review. Each data breach incident will be reviewed, and the response tailored to the circumstances of the event.

REFERENCES - INTERNAL

- Consent Policy
- Data Breach Management Response Plan Procedure
- Information Communication & Technology Policy
- Records Management Policy

REFERENCES - EXTERNAL

- Charter of Human Rights and Responsibilities Act 2006
- Disability Act 2006 (Vic)
- Freedom of Information Act 1982
- Health Records Act (2001) (Vic)
- Health Records Act 2001 (Vic.).
- Information Privacy Act (2000) (Vic)
- Notifiable Data Breach Scheme.
- Privacy Act 1988 (Federal).
- Privacy and Data Protection Act 2014 (Vic.).

REVIEW

Alkira at its own discretion reserves the right to change the policy and procedure in line with relevant legislation, organisational needs and review schedule. This document remains current until next reviewed.

If this policy can be improved, please submit a suggestion for improvement to the Quality Department using the Improvement Matters Form on the Alkira staff intranet or email feedback@alkira.org.au

VERSION CONTROL

Authorised by:	Chief Executive Officer
Policy Owner:	Board of Directors
Date of Approval	21/03/24
Next Review Due	21/03/27