PRIVACY AND CONFIDENTIALITY POLICY

including NDIS requirements

Supporting Policy

Policy ID Reference Number

SPOL-GOV-1-107

POLICY DETAILS

Policy ID:	**SPOL-GOV-1-107**
Core Policy:	**Governance**
Author:	**CFO**
Reviewer:	**CEO**
Approver:	**CEO**
Applies to:	**All Directors and employees**
Review Cycle (years)	**1 Year ***
Due for review:	**30/10/2024**

***Requirement of NDIS SDA**

DOCUMENT VERSION HISTORY

Version No.	Effective Date	Author Name, Position	Version Change/Description	Reviewer Name, Position	Date Approved	Signature / Position of Approver
0.1	24/05/2014	Coast2Bay	Initial Policy	Board	23/15/2014	Board
0.2	18/12/2017	Lisa Beaton	Updated Policy	Board	18/12/2017	Board
0.3	01/08/2018	Jo Ahern	Initial Draft	CEO	01/08/2018	
0.4	08/10/18	Jo Ahern	Second Draft	CEO	08/10/18	
0.5	05/11/2018	Jo Ahern	Third Draft to Andrew Elvin for Review	CEO	05/11/2018	
0.6	12/11/2018	Andrew Elvin, CEO	Final Draft	Board	12/11/2018	Board
1.0	18/12/2018	Andrew Elvin, CEO	Final Version (following Board amendments)	Board	18/12/2018	Board
2.0	30/10/2023	Lynda Delaforce, CFO	New format and full review	CEO	30/10/2023	Board

DISCLAIMER

The content of this document is correct as of the Effective Date and is subject to change at regular review intervals. Any reference to legislation, regulation, industry standard or code includes any modifications or substitutions that may occur after the Effective Date. It is the responsibility of all C2B Directors and Employees to understand and comply with this policy and accompanying procedure at all times.

CONTENTS

1 SCOPE

Coast2Bay Housing Group (C2B) is committed to establishing and continually reviewing a clear and consistent set of policies and procedures. These are to be in line with legal and regulatory frameworks and will control the activity of the company.

The Board of Directors, staff (and volunteers) are committed to protecting the privacy of all personal information obtained by the organisation.

This policy is implemented to ensure the entity's ongoing compliance with the *Privacy Act 1988 (Clth*) and the National Privacy Principles (NPPs).

This policy must be followed by Directors, the Executive, Managers and employees of the company.

2 OBJECTIVE

The objective of establishing this supporting policy is to provide the framework through which the Board and CEO govern and manage the organisation's privacy and confidentiality policy and day to day functions to protect and secure personal information. It also aims to ensure the following:

- That Board confidentiality is critical to open and frank discussions at meetings, facilitation of the organisation's vision and implementation of its strategy and policy
- That Board confidentiality protects information that is confidential, personal, or relates commercial, legal or employment matters.
- That the Board and all staff protect the personal information that has been collected from tenants, landlords, stakeholders, clients, staff and any other person subject to the data that has been collected meets the definitions under this policy.

3 DEFINITIONS

Privacy laws do not regulate or apply to all information gathered by not-for-profit organisations. There are three types of confidential information under privacy laws including:

- personal information
- sensitive information
- health information.

National Privacy Principles (NPP)	means a national privacy principle stated as a section of schedule 4 of the *Information Privacy Act 2009 (Qld).*
Personal information	is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Examples include: a person's name, address, contact details, date of birth, gender, sexuality, race / ethnicity. Note that in respect of a data breach involving personal information is likely to result in serious harm, please refer to notifications policy.
Sensitive information	about an individual, for the NPPs, means—

	(a) personal information about the individual that includes any of the following— (i) the individual's racial or ethnic origin; (ii) the individual's political opinions; (iii) the individual's membership of a political association; (iv) the individual's religious beliefs or affiliations; (v) the individual's philosophical beliefs; (vi) the individual's membership of a professional or trade association; (vii) the individual's membership of a trade union; (viii) the individual's sexual preferences or practices; (ix) the individual's criminal record; or (b) information that is health information about the individual for the NPPs
Health information	about an individual means (a) personal information about the individual that includes any of the following: (i) the individual's health at any time; (ii) a disability of the individual at any time; (iii) the individual's expressed wishes about the future provision of health services to the individual; (iv) a health service that has been provided, or that is to be provided, to the individual; or (b) personal information about the individual collected for the purpose of providing, or in providing, a health service; or (c) personal information about the individual collected in connection with the donation, or intended donation, by the individual of any of the individual's body parts, organs or body substances. Examples include physical and mental health, disabilities, health preferences, use of health services, implants, organ donation, genetics.

4 PRINCIPLES

4.1 Overview

The organisation is committed to achieving its strategic purpose, priorities and objectives.

The following sets out principles that guide the Board's and CEO's leadership and management of the organisation:

- Australian Privacy Principles
- Commercial in confidence, legal and employment matters
- Compliance with law, policy, procedural fairness and natural justice
- Funder/ Investor agreements and contracts
- Risk mitigation and treatment
- Stakeholder communications and engagement regarding how personal data is stored and/or can be used/ disclosed and accessed
- Understanding charitable purpose and duties in managing confidentiality

5 PRIVACY

5.1 Overview - Collecting and protecting personal information

Personal information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable.

All personal information will be collected in accordance with the following guidelines:

- Only relevant and necessary personal information will be collected
- Confidentiality will be maintained regardless of the method used to collect the personal information
- Personal information will be collected in a fair, legal and transparent way
- Reasonable steps will be taken to collect personal information in a private and secure manner

Personal information will be restricted to authorised persons only and for the purpose it was collected.

Personal information will only be disclosed with consent from the individual or for a 'permitted general situation' as defined by the Office of Australian Information Commissioner (OAIC).

A legal representative may be in place to provide consent on behalf of an individual. The entity will ensure evidence of this is obtained and kept on the relevant file.

Individuals reserve the right to withdraw consent at any time. This will be recorded on the relevant file to ensure information is not disclosed. Information disclosed external to the entity is considered uncontrolled and staff will take reasonable steps to ensure information will be kept confidential.

The entity will provide an individual access to their personal information unless there are grounds for refusal as per the NPPs.

Where access to personal information has a financial impact on the entity, reasonable costs may be recovered from the individual at the discretion of management.

The entity will take all reasonable steps to ensure the security of personal information, and to ensure that information is kept up to date. Any changes to information will be processed as soon as practicable. Personal information will be maintained in a secure manner at all times within the entity's protected systems with strict access subject to both passwords and dual authentication.

Personal information that is no longer required to be kept by the entity will be destroyed or de-identified, as required. This will be done in a secure manner to ensure the information is irretrievable.

The entity will take immediate and appropriate action in the event of a suspected data breach pursuant to the Cyber Incident Response Plan.

All suspected data breaches/incidents will be managed in accordance with the CIRP and other ICT policies as relevant. The CIRP includes many aspects including investigation, containment of the breach, assessment of the incident, notification and review in a formalised manner.

The entity will notify the OAIC, relevant bodies (as required) and individuals of a data breach involving personal information that is likely to result in serious harm as identified in the CIRP.

Privacy and confidentiality documents are read and signed by Directors, staff, volunteers and relevant stakeholders upon induction and annually.

The entity will ensure staff are adequately trained and provided up to date information regarding their privacy and confidentiality obligations. Records of training will be maintained.

Failure to comply with the entity's Privacy and Confidentiality obligations will be taken seriously and is considered a breach of conduct. This may result in disciplinary action.

5.2 How information is collected

The entity may collect personal information by:

- directly over the phone or via our Customer Services staff
- contact in person
- participate in public or closed surveys, questionnaires or conference events
- register for face-to-face or digital events (such as webinars, fundraisers)
- interact with us online, including through our websites, email, webchats, mobile applications and social network services (such as Facebook, Twitter, YouTube, Instagram or LinkedIn – the social network providers will also handle your personal information for their own purposes and have their own privacy policies)
- and individual donating to the organisation and have consented to receiving information for future fundraising
- and individual applying for a position with the entity (either as an new board member, employee, or as a volunteer or as a contractor).

This collection may be required to allow several activities to be conducted in the normal course of business including:

- making a donation or participating in a fundraising event
- receive information from the entity including alerts via email or SMS communications
- being a shareholder
- being a member of a community organisation that the entity is engaged with
- registering as a volunteer
- register as a RISE Ambassador or Speaker or committee member
- being a debtor (owing money to the entity) or being a creditor (being owed money by the entity)
- participate in tenancy and community engagement activities and programs
- being subject to involvement with any business program (including government funded programs)
- being a tenant or ex-tenant in one of our properties that we own or manage on behalf of others
- being an investor or client who has a headlease or provided outsourced servicing to the entity to manage their property(s).
- receive information about or become involved in our programs, campaigns or other initiatives
- use our mobile applications
- register with centrepay and other government support services
- would like to or will be appointed as an employee with information collected in relation to paying the employee for services and facilitation of superannuation, PBI and employee leave entitlements.

5.3 Third party information

There may be occasions when the entity gathers personal information about an individual from a third party, for example, from recruitment services, community groups and government support providers, IT or telecommunications provider or our delivery partners. These third parties also have their own privacy policies.

5.4 Sharing our stories

If staff or the Board want to share a story that includes another person's experience of anxiety, depression or another other concern and where a successful outcome as a result of such an experience has occurred, in which that person will be identifiable, then the entity must have proof that permission from the individual or next of kin was sought first. The individual must be advised of our Privacy Policy. In addition, some people may not want their experience made public, particularly if one person's story (with consent) mentions other individuals. It is important to consider the impact and respect the wishes of others affected by the same story.

5.5 How personal information is used

The personal information you collected by the entity may be used by us for the following purposes:

- managing preferences for receiving further information about the entity's programs, events, campaigns or activities;
- additional types of personal information such as job title or role, department name, educational institution information; and
- demographic information and unique identifiers in order to provide clients with a more personalised experience and to verify who the client is
- ensuring a lease arrangement for housing is in place
- to allow you to obtain access to the interactive elements of our mobile applications and websites (including the online forums, our campaign websites etc.)
- to provide stakeholders with the information, resources or merchandise they have requested
- to involve clients in programs, campaigns, research, activities or other initiatives undertaken
- to show the donators name and the amount of any donation or sponsorship that they may wish to may make on our website (unless chosen to be a private or anonymous donation)
- for the marketing and research purposes of the entity, its contractors or service providers
- for internal administrative purposes
- to respond to 'Contact Us' form enquiries, general website feedback or assistance, or media enquiries
- to update our records and keep client contact details up to date
- for research, advice and information, including for benchmarking purposes
- to send emails about our programs, campaigns or activities if stakeholders have agreed to receive our emails
- in the case of marketing automation, to improve the emails that are sent to donators and to improve the personalisation, services, programs, content and resources that are offered to them
- to understand how stakeholders interact with us by recording information about them in a database
- to enable like-minded organisations to contact our client with information that may be of interest to them (if they have consented to this)
- to assess any application from relating to a vacant position
- if you lodge a complaint or query with the entity, and then to process and respond to that complaint or query.

Other than for the purposes described above, the entity will not use personal information without their prior consent.

5.6 Disclosure of personal information

Personal information will only be disclosed to third parties in accordance with this Policy or as permitted by law.
The entity will only use or disclose your personal information for the purposes for which it has been collected or for a secondary purpose if permitted by law, which includes:

- where have consent has been received
- where it is reasonably expected of the entity to do so, and where related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
- where required or authorised by or under an Australian law or a court/tribunal order
- where a permitted situation exists under the Privacy Act, such as lessening or preventing a serious threat to the life, health or safety of an individual, or to public health or safety, or locating a person reported as missing.

Information may be provided to third parties where services relating to the purpose for which the personal information is collected are outsourced or you would reasonably expect us to disclose it to a third party for a particular purpose. For example, we may disclose your personal information to:

- our service support providers
- our delivery partners
- our third-party service providers (such as our IT and maintenance contractors)
- our marketing team
- our professional advisors (such as accountants, auditors and legal representatives)
- pending on the formal provisions of terms and conditions within our contracts with government, information pertaining to community housing statistics and other reportable data

Our third-party service providers may store personal information overseas when providing support or other services. For example: If a stakeholder has communicated with us through a social network service such as Facebook or Twitter, the social network provider and its partners may collect and hold their personal information overseas.

5.7 Accessing personal information

Stakeholder may request access to their personal information collected by the entity and ask for correction or update of that personal information. They can ask for access or correction by contacting us and we will usually respond within a very reasonable time. If there is a refusal to provide access to, or correct, their personal information, the entity will notify them in writing setting out the reasons.

5.8 Notifiable data breach

In the event of any unauthorised access or unauthorised disclosure or loss of a stakeholders personal information that is likely to result in serious harm to them, and where remedial action has not been able to prevent the likely risk of serious harm, the entity will investigate and notify them and the Office of the Australian Information Commissioner in accordance with the *Privacy Act 1988.* Refer to Notifications Policy in respect of how to report a data breach of notifiable data breaches..

6 CONFIDENTIALITY

6.1 Overview of confidentiality

Board members must keep confidential all information pertaining to matters dealt with by the Board. This includes board papers (meeting minutes, agendas, reports and associated documents, and information contained in such documents). Particular emphasis on confidentiality is key when matters are considered commercial in confidence in accordance with the requirements of the Information Privacy Principles (Schedule 3, *Information Privacy Act 2009 (Qld)*).

The Board's obligation to maintain confidentiality continues to apply even after a Director has left the organisation. Maintaining confidentiality also ensures that Board members observe their legal duty:

"A person who obtains information because they are, or have been, a member of the Board must not improperly use the information to:

- *gain an advantage for themselves or someone else; or*
- *cause detriment to the organisation."*

If a request is made for access to one or more Board Papers, the Board may, on a case by case basis resolve to provide access to the document/s.

In considering this, the Board will review:

- The importance of maintaining confidentiality to facilitate effective board meetings
- The importance of complying with the law – including privacy law - recognising that law sometimes creates duties to disclose or protect information
- Whether the person requesting the document is a member, and the important role of members in holding the Board accountable
- The need to be consistent in the way documents are treated and consequence of establishing precedents or expectations.
-

Nothing in this policy prevents the Board from seeking confidential legal, accounting, financial or other expert advice from independent professionals to assist in carrying out its responsibilities.

Any officer (the CEO & Company Secretary and CFO), who is not a member of the Board but is present at Board meetings or parts thereof, must maintain the confidence of all information obtained as a result of participation in a meeting.

In addition, the privacy of clients, staff and members of the organisation will be respected. Information obtained in the course of professional conduct of the organisation will be held in confidence in accordance with the requirements of the Information Privacy Principles (Schedule 3, *Information Privacy Act 2009(Qld)).*

The organisation will collect, store, secure, access, amend, use, disclose and ensure the accuracy of personal information in accordance with the Information Privacy Principles.

Board Directors and employees are expected to work cooperatively, to maintain confidentiality, offer one another support and to view their work as part of a team effort directed towards the overall goals of the organisation, its vision, mission and values.

Duty of Care is the level of competence expected of a Director, the CEO & Company Secretary, Public Officer or Executive Team, commonly expressed as the duty of care an ordinary prudent person would exercise in a like situation under similar circumstances.

The duty of care of all staff persons is to ensure that all foreseeable risks relating to their duties (data management, property management, tenancy management, office practices, client interactions etc.) are minimised or avoided.

Duty of Loyalty is a standard of faithfulness a Director the CEO & Company Secretary and Public Officer must give to Coast2Bay when making decisions. Directors, the CEO & Company Secretary and Public Officer must always act in the best interests of the organisation and never use information obtained in the course of their duties for personal gain.

6.2 Limitations to Confidentiality

Maintaining client confidentiality provides the client with safety and privacy and protects their autonomy.

There are however, exceptional circumstances in which the Board or CEO & Company Secretary may be satisfied that there are reasonable grounds on which disclosure is necessary:

- To lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare
- For reasons of law enforcement.

In such circumstances a decision to break confidentiality should be:

- discussed with the client in consultation with the relevant Executive Manager or Chair
- restricted to relevant information, conveyed only to appropriate people and for appropriate reasons, with the aim of alleviating the exceptional circumstances
- given to achieving a balance between acting in the best interests of the client and the worker's responsibilities to the wider community.

All Directors and staff are responsible for complying with this policy.

6.3 Requirements for the Board and Staff

The Board shall ensure that:

- Directors individually sign a Consent and Disclosure form upon appointment to the Board of Directors
- where release of any material would involve the unreasonable release of personal information regarding any person, may
    - declare that material to be confidential, or,
    - if appropriate, remove identifying material from the material before release
    - be authorised to release to any person any material that has not been ruled by the Board to be confidential
- for those matters that the Board elects not to make public, Board Directors shall respect the confidentiality of those documents and of any deliberations in the Board on those matters.
- The obligation to protect such confidential matters from disclosure continues even after the individual Board member is no longer serving on the Board
- Where appropriate, observers may be admitted to Board meetings subject to their undertaking to maintain confidentiality
- Where appropriate, remove information identifying individuals from material before its consideration by the Board, or may be removed from material before it is released.

The CEO shall ensure that Employees (including volunteers)

- sign a confidentiality statement on commencement with the company.
- are aware of their obligations to demonstrate professional conduct and duty of care in all their dealings for and on behalf of the organisation.

- shall respect the confidentiality of information obtained in any meetings, collection of personal information or other dealings within the organisation and will not disclose to any person or organisation any information concerning the personal details, circumstances or affairs of individuals who are clients, participants or employees of the organisation.
- are aware that breaches of confidentiality are treated as a disciplinary matter
- will ensure that all verbal, written or electronic information regarding any tenant or client of the organisation will remain confidential to the organisation, and may not be shared without the expressed or written consent.
- must adhere to the Funding Guidelines and Legislation relevant to the organisation.
- must evidence a Duty of Loyalty as a standard of faithfulness when making decisions on behalf of the organisation.
- must ensure that all communication between agencies about a tenant, applicant or client must be with the clients consent and must be mindful of confidentiality and privacy policy and procedures.

It is also the responsibility of the Board and CEO to:

- Ensure Board materials are appropriately classified as confidential when appropriate
- Ensure the three types of information (below) are covered by privacy law are managed in accordance with the laws and good governance and systems satisfy those laws regarding collection and protection. (refer section 3 Definitions)
    - Personal information
    - Sensitive information
    - Health information

In addition to the definitions, important information relating to collecting and keeping information confidential and secure is relevant as follows:

- Deceased persons do not have personal information under federal privacy laws although in some states / territories this information requires protection for a period of time; and when it concerns a living person. Regardless, all information relating to a client who is deceased should be removed and any information regarding that individual kept confidential.

Personal information does not include:

- that which is anonymous
- aggregated information (e.g., data that reflects trends without identifying a sample)
- de-identified data
- information about companies or other entities that does not identify an individual.

Personal information that is not collected for a ‘record’ will be outside the scope of privacy laws (e.g., what a person did on the weekend). However, if such information is collected for the purposes of recording it; it may well be subject to privacy laws, and confidentiality thereof should continue.

Other information that can identify a person and if not kept or managed properly, could result in legal action should there be a case of identity thief. This includes but is not limited to:

- spent convictions (old, minor criminal convictions)
- tax file numbers
- date of birth, place of birth
- photographs of individuals and their kin
- drivers licence and passport information
- medicare care details
- centrelink details
- mygov details
- electoral roll information
- surveillance information
- credit history.

Legal action would be a real and actionable risk in respect of breach of such other information collected by the entity, particularly in respect of cyber espionage. Confidentiality of any such information is also required.

7 RESPONSIBILITIES

The Board Chair is responsible for ensuring the Board and Directors are aware of this policy and relevant procedures.

The CEO is responsible for ensuring the Executive Team and employees are aware of this policy and relevant procedures.

The Board of Coast2Bay Housing Group will delegate the development and renewal of accompanying procedures to the CEO and Executive Team (Chief Finance Officer (CFO) and Chief Operations Officer).

The Executive Team will ensure that accompanying procedures will be developed and regularly reviewed at least every three years.

8 CHANGES TO THIS POLICY

This Policy may change from time to time. Any updated versions of this Policy will be reviewed by the Board of Directors.

9 RELATED DOCUMENTS / PROCEDURES

ID	Name
PMAN-GOV-1-101	Governance Policy Manual
CPOL-GOV-1-001	Governance Core Policy
SPOL-GOV-1-102	Code of Conduct
SPOL-GOV-1-103	Delegations of Authority
SPOL-GOV-1-104	Finance Audit and Risk Committee Charter
SPOL-GOV-1-106	Conflict of Interest Policy
SPOL-GOV-1-108	Anti-Fraud, Anti-Corruption and Misconduct Control Policy
SPOL-GOV-1-109	Notifications Policy
SPOL-GOV-1-112	Whistleblowing Policy
PROC-GOV-1-208	Notifications & SDA Incident Management Procedure
SPOL-ORG-2-117	Gifts and Fundraising Policy
	Cyber Incident Control Plan

10 LEGISLATIVE COMPLIANCE

Coast2Bay Housing Group adheres to a wide range of legislation, regulation and codes of practice in its governance control systems, policy and procedures. Details of these can be found in the Governance Core Policy.

This policy is drafted in compliance with all relevant national and state legislation, standards and codes. In particular, those relating to landlord, tenancy, building, health and safety and NDIS SDA requirements.