



Confidentiality Policy

Prepared 30 September 2026

Applies across ABB's NDIS services, community programs, cultural activities, workshops, social enterprise and other organisational activities.

1. Purpose

Ability Beyond Boundaries Ltd (ABB) respects the privacy, dignity and safety of everyone involved in its work. This policy explains how ABB's representatives must protect confidential information and how people can raise concerns. It supports trust, informed choice and respectful service delivery.

2. Scope

This policy applies to board members, employees, contractors, volunteers, students on placement, advisors and others acting on ABB's behalf. ABB must establish appropriate confidentiality obligations with suppliers and partners who receive confidential information.

It protects information about NDIS participants, community members, families, carers, staff, volunteers, donors and other stakeholders, as well as confidential organisational information. It applies to information held verbally, on paper, electronically, in images or recordings, and through online services.

3. What is confidential information?

Confidential information includes personal information, service and support records, assessments, health and disability information, identity documents, financial details, complaints, safeguarding matters, and private information entrusted to ABB by others. It also includes non-public business plans, contracts and internal records where confidentiality is appropriate.

Sensitive personal information includes health information and information about matters such as racial or ethnic origin, religious beliefs and sexual orientation. Identity documents and financial records must also be carefully protected, even where they are not legally defined as sensitive information.

4. Responsibilities

Everyone covered by this policy must use confidential information only for authorised duties, access only the information they need, follow secure handling practices, and report suspected breaches promptly. The Executive Director oversees implementation; the Board oversees accountability and concerns involving senior management.



5. Collecting and using personal information

ABB must collect only information reasonably necessary for its activities and explain the purpose of collection in an accessible way. Information must be used for the purpose for which it was collected, or another purpose permitted by applicable law. Sensitive information must be collected with informed consent unless a lawful exception applies.

Where practicable, information should be collected directly from the person. If it is obtained from a representative, referral source or other organisation, ABB must check the authority or lawful basis for doing so. Confidential information must not be used for personal purposes, gossip or unauthorised publicity.

6. Consent and supported decision-making

Consent must be informed, voluntary, specific and current. ABB must explain what information will be shared, with whom and why, and record consent where appropriate. Communication support or an interpreter should be arranged where needed. A person may withdraw consent for future optional sharing; ABB must explain any effect this has on services and any information it must retain or disclose by law.

A family member or carer does not automatically have authority to consent or access records. ABB must verify a representative's authority and its scope, respect the person's own choices, and support their involvement in decisions. Consent involving children must take account of capacity, lawful parental or guardian authority and applicable requirements.

7. Sharing information

Internal access must be limited to authorised people who need the information for their duties. External disclosure must have a lawful basis, such as informed consent or a requirement or permission under applicable law. ABB must share only the information reasonably necessary and use appropriate security and confidentiality arrangements.

There may be circumstances where information can or must be disclosed without consent, including applicable reporting obligations, court orders or a lawful exception relating to a serious threat to life, health or safety. ABB must verify and document the basis for disclosure. An internal safeguarding procedure alone does not authorise disclosure, and a confidentiality agreement alone does not provide a lawful basis to share personal information.

8. Photographs, recordings and personal stories

ABB must obtain specific informed consent before using identifiable photographs, recordings, testimonials or personal stories in publicity, on its website or on social media. Agreement to receive services or attend an activity does not itself provide publicity consent. Declining optional publicity must not disadvantage a person's access to services.

People must be told the intended use and audience. Withdrawal must be respected for future use, with an explanation that ABB may not be able to retrieve copies already distributed or shared by others. Event photography arrangements must offer a practical way for people to express their preferences.



9. Storage, communication and disposal

ABB must take reasonable steps to protect information from misuse, interference, loss and unauthorised access, alteration or disclosure. Paper records must be secured; electronic records must have appropriate access controls, passwords and security protections. Encryption and additional controls must be used where appropriate to the risks.

Representatives must use ABB-approved systems, check recipients before sending information, and avoid discussing private matters where others can overhear. Personal accounts, unapproved devices and online tools must not be used for confidential records without explicit organisational authorisation and appropriate safeguards.

Records must be retained for applicable legal, contractual and service requirements. When no longer required and lawful to dispose of, paper records must be securely destroyed and electronic records securely deleted or de-identified as appropriate. Disposal must account for copies and backups. Information must not be destroyed to obstruct a complaint, investigation or lawful reporting.

10. Access, correction and concerns

People may ask ABB to access or correct their personal information by contacting the Executive Director through ABB's published Contact details. ABB must verify identity, assess the request under applicable law, respond within applicable timeframes, and explain any lawful refusal and available review or complaint options.

Privacy or confidentiality concerns may be raised verbally or in writing through the same channels, with communication support or an advocate if requested. Concerns about the Executive Director should be referred to the Board Chair or another unconflicted director. ABB must handle concerns fairly, protect information on a need-to-know basis, explain the outcome and avoid retaliation.

External concerns about NDIS supports may be raised directly with the NDIS Quality and Safeguards Commission (www.ndiscommission.gov.au). Privacy complaints may be raised with the Office of the Australian Information Commissioner where it has jurisdiction (www.oaic.gov.au).

11. Breaches, training and continuing obligations

Actual or suspected unauthorised access, disclosure or loss must be reported promptly to the Executive Director, or to an unconflicted director where appropriate. ABB must contain the incident, assess harm, keep appropriate records and take corrective action. Affected people and regulators must be notified where applicable legal notification thresholds and requirements are met. Not every confidentiality breach is automatically reportable to the NDIS Commission.

ABB must provide induction and appropriate refresher training, monitor compliance and address breaches fairly. Action may include corrective training or disciplinary or contractual measures, consistent with applicable law. Confidentiality obligations continue after a person's employment, placement or engagement ends. This policy does not prevent lawful protected disclosures or reporting concerns to regulators.

12. Policy review

Policy owner: Executive Director. Prepared: 30 September 2026. Review cycle: every two years, or sooner following a significant incident or change in law or operations.