



1. Introduction

1.1. Purpose

The purpose of the Privacy and Information Management Policy for Defuse Behaviour Solutions, an NDIS service provider, is to establish clear guidelines for collecting, using, storing, disclosing, and disposing of participants' information and to protect their right to privacy. It aligns with the Privacy and Dignity and Information Management NDIS Practice Standards, Australian Privacy Principles, and relevant laws.

1.2. Scope

This Policy is applicable to all Employees affiliated with Defuse Behaviour Solutions. Every individual, regardless of employment status, is responsible for fully understanding and complying with the commitments outlined in this policy. All Employees must acknowledge that they have read, understood and will comply with the contents of this Policy.

1.3. NDIS Indicators (Objectives)

Privacy and Dignity

Outcome: Each participant accesses supports that respect and protect their dignity and right to privacy.

To achieve this outcome, the following indicators should be demonstrated:

- a) Consistent processes and practices are in place that respect and protect each participant's personal privacy and dignity.
- b) Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant employees.
- c) Each participant understands and agrees to what personal information will be collected and why, including recorded material in audio and/or visual format.

Information Management

Outcome: Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant employees.

To achieve this outcome, the following indicators should be demonstrated:

- a) Each participant's consent is obtained to collect, use and retain their information or to disclose their information (including assessments) to other parties, including details of the purpose of collection, use and disclosure. Each participant is informed in what circumstances the information



could be disclosed, including that the information could be provided without their consent if required or authorised by law.

- b) Each participant is informed how their information is stored and used, and when and how they can access or correct it, and withdraw or amend their prior consent.
- c) An information management system is maintained that is relevant and proportionate to the size and scale of the organisation and records each participant's information accurately and in a timely manner.
- d) Documents are stored with appropriate use, access, transfer, storage, security, retrieval, retention, destruction and disposal processes relevant and proportionate to the scope and complexity of supports delivered.

2. Policy Statement

At Defuse Behaviour Solutions, we are deeply committed to safeguarding our Participants' right to privacy while ensuring accurate, reliable, and accessible management of their information. We believe that every Participant's personal data should be treated with utmost respect and confidentiality. This policy guides our practices towards these commitments, underpinning our organisational principles of respect for Participant autonomy, transparency, and accountability. It establishes the standards for our dedicated workforce to handle information appropriately, respecting each Participant's privacy and dignity.

2.1. Relevant legislation

All relevant legislation to this Policy is outlined in the Legislation Register.

2.2. Related documents

- a) Privacy Consent Form
- a) Privacy Consent Form (Easy Read)
- b) Incident Management Policy
- c) Incident Report Form
- d) Feedback and Complaints Policy
- e) Risk Management Register

3. Responsibilities and Roles

- a) Esme Jorgensen is responsible for developing and reviewing this policy. Esme Jorgensen is expected to ensure this Policy remains compliant with all applicable laws, regulations, and standards.
- b) Key Management Personnel play a vital role in ensuring the effective implementation of this Policy throughout Defuse Behaviour Solutions. All Key Management Personnel are responsible not only



for assisting Employees in understanding and complying with this policy, but also for complying with it themselves. Leading by example, they demonstrate the importance of adherence to the policy and foster a culture of compliance within the organisation.

- c) Employees are responsible for understanding this policy and complying with all procedures applicable to them.

4. Definitions

Defuse Behaviour Solutions means Defuse Behaviour Solutions Pty Ltd ABN 67700401369.

Key Management Personnel means Esme Jorgensen and other key management personnel involved in Defuse Behaviour Solutions from time to time.

Director means Esme Jorgensen.

Worker or Employee means a permanent, fixed-term or casual member of staff, a contractor or volunteer employed or otherwise engaged by Defuse Behaviour Solutions and includes the Director.

Personal information means any data or viewpoint about an identifiable individual or one who can be reasonably identified, regardless of the veracity of such information or if it is recorded in a physical form.

Sensitive information means a category of personal information that usually receives a higher degree of privacy protection. This encompasses details related to health, genetic makeup, racial or ethnic background, political viewpoints, association with a political group, religious or philosophical beliefs, affiliation to a professional or trade association or union, sexual orientation or behaviour, criminal history, and certain kinds of biometric information.

5. Procedures

5.1. Protection of Sensitive Information

- a) As part of Defuse Behaviour Solutions' Privacy and Information Management Policy, we carefully manage sensitive information to protect the privacy and dignity of our participants.
- b) Defuse Behaviour Solutions only collects sensitive information where it is reasonably necessary for our functions or activities. This could include health and medical information and information relating to disability and support requirements. This will only be done under two circumstances:
 - 1) The individual has given explicit consent.
 - 2) Defuse Behaviour Solutions is required or authorised by law, including applicable privacy legislation, to do so.



- c) Defuse Behaviour Solutions is committed to treating all Participants with dignity and respect. We take all reasonable measures to protect the privacy and dignity of each participant, particularly when handling their sensitive information.

5.2. Obtaining Participant consent

- a) Employees must, in a respectful, clear, and honest manner, explain to the Participant the purpose and potential use of their data, and who it may be disclosed to, including instances where information may be shared without consent, as required by law.
- b) Employees should use plain language, active listening, and encourage questions to ensure the Participant fully understands.
- c) Consider any potential communication barriers and the efforts made to address them, for instance by offering interpreter services or legal aid.
- d) Employees must document the Participant's consent using the Privacy Consent Form, ensuring the Participant fully understands and agrees to all details.

5.3. Informing Participants about their information

- a) Employees must inform Participants about their data storage and usage. This should be done when providing the Privacy Consent Form during the initial intake process, and periodically thereafter, or when data storage or usage changes.
- b) Communications should respect the Participant's privacy and confidentiality.
- c) Employees should provide information on how Participants can contact Defuse Behaviour Solutions to access or correct their data, lodge a complaint, or amend their prior consent.
- d) If the Participant wishes, Employees should encourage their engagement with family, friends, or chosen community in this process.
- e) If a Participant has a complaint about how Defuse Behaviour Solutions has collected or handled their personal information, it will be managed in accordance with the Defuse Behaviour Solutions Feedback and Complaints Policy.

5.4. Information collected and stored

- a) The personal information Defuse Behaviour Solutions collects and securely stores includes:
 - 1) Participant Details including Name, contact details, gender, date of birth, marital status, disability and support needs.
 - 2) Identifiers such as Numbers used by the government or other organisations for identification.



- 3) Service Details such as Information about provided services and delivery methods.
 - 4) Medical Information including Health and medical details relevant to service provision.
 - 5) Financial Information including billing details and information about funded services under NDIS or otherwise.
 - 6) Interaction Records including records of conversations and interactions with our employees.
- b) Defuse Behaviour Solutions may collect personal information in the form of recorded material such as audio and/or visual format.

5.5. Information collection methods

- a) Defuse Behaviour Solutions collects personal information through various means to ensure the effective delivery of our services. These methods include:
- 1) Information provided through forms, website, or online interactions (if applicable).
 - 2) Information gathered when individuals correspond with us, for example via letters, faxes, emails, or telephone calls.
 - 3) Personal data collected through forms filled out in-person or received via mail.
 - 4) Information collected directly during face-to-face interactions.
 - 5) Information obtained from referring third parties, such as the National Disability Insurance Scheme or a support coordinator.
 - 6) Personal information collected from participants during events and forums.
 - 7) Personal information received from third-party funding and Government Agencies.

5.6. Purpose of personal information collection

- a) As an NDIS service provider, Defuse Behaviour Solutions collects personal information to manage, provide, and enhance our services. This data collection enables us to:
- 1) Understand and evaluate Participants' specific needs, preferences, and goals to customise Participant Support plans.
 - 2) Answer Participant inquiries, administer services, process payments, and provide tailored supports as per the Participants' NDIS plans.
 - 3) Keep Participants updated about their plans, our services, and any changes or updates, including information about disability supports and the NDIS.



- 4) Carry out quality assurance activities, including surveys, research, and analysis; resolve complaints; and continually refine our services to meet the NDIS Practice Standards and Quality Indicators.
- 5) Adhere to legal, regulatory, and reporting obligations, including incident reporting, record-keeping, and providing reports to funding and government agencies.
- 6) Inform individuals about our activities and promote Defuse Behaviour Solutions, including through events and forums. Where consent is provided, we may send marketing communications.
- 7) Perform research and statistical analysis relevant to our services, and invite individuals to participate in these activities, which contribute to evaluating and enhancing our services.
- 8) If applicable, manage and improve user experience on our website using “cookies” to personalise webpage content, track visits, and tailor advertising. Users can manage cookies through their browser settings.

5.7. Third party disclosures

- a) Defuse Behaviour Solutions may share personal data with certain third parties including:
 - 1) NDIS Commission;
 - 2) funding providers;
 - 3) regulatory bodies like National Disability Insurance Agency, and Medicare;
 - 4) individuals acting on the subject's behalf;
 - 5) law enforcement;
 - 6) courts;
 - 7) financial institutions for payment processing; and
 - 8) External service providers.
- b) These disclosures are made to fulfil our services, comply with laws, or at the subject's explicit authorisation.

5.8. Maintaining the Information Management System

- a) Employees responsible for handling information must ensure information is entered into the Defuse Behaviour Solutions document management system (Halaxy) accurately and on time.
- b) Management should perform regular system audits to ensure information is kept current and accurate.



5.9. Document storage and security

- a) Defuse Behaviour Solutions ensures the security of personal information via several strategies, including:
- 1) website encryption;
 - 2) two-factor authentication (2FA)
 - 3) firewalls;
 - 4) restricted system access with password protection;
 - 5) controlled physical access to premises;
 - 6) limiting data access to necessary Employees; and
 - 7) providing ongoing data security training and policies.
- b) All documents, electronic or paper-based, must be stored in accordance with the following document storage and security procedures. This includes appropriate use, access, transfer, security, retrieval, retention, and disposal.

1) Storage

- (i) All electronic-based documents are stored in a cloud-based storage system (Google & Halaxy).
- (ii) All paper-based documents should be converted into an electronic version and uploaded to the company's Google Drive storage system; the paper-based documents should be stored in a locked file cabinet or destroyed.

2) Transfer of documents

- (i) Ensure necessary consents have been obtained before transferring any document containing personal or sensitive data.
- (ii) All confidential documents (physical or digital) should be clearly marked as "Confidential."
- (iii) For internal document transfers: digital transfers should use secure, approved, company-controlled systems (like an intranet or secure shared drives), and access should be restricted to only those who need it. Transfer physical documents directly hand-to-hand wherever possible. If this is not feasible, use internal mail services with a traceable delivery process.
- (iv) For external document transfers: digital transfers should preferably be encrypted before transmission and use secure, approved methods (like secure email, secure file transfer protocol (SFTP), or encrypted cloud services). Share the encryption key/password via a separate, secure communication method. For sending physical documents outside of the organisation, use a reliable



courier service that offers secure, traceable delivery. Pack documents in tamper-evident packaging.

3) Information Retention

- (i) Once their defined retention periods end, we will dispose of all physical and electronic documents in accordance with our document disposal procedures to ensure safe, confidential elimination.
- (ii) Unless mandated differently by legal requirements, all records and personal information of our Participants will be preserved for the following durations:
 - a. For adult Participants: A minimum of seven years after they cease to be Participants of Defuse Behaviour Solutions.
 - b. For minor Participants: For Participants who were under 18 years of age when they received services from Defuse Behaviour Solutions, records will be retained until the Participant reaches 25 years of age.

4) Disposal of Information

During the disposal process, Employees should abide by the following steps:

- (i) Determine if the documents have reached their designated end of the retention period. Ensure that there are no pending requests or legal obligations for these documents.
- (ii) Assign a classification to the documents based on the nature of their contents and the level of confidentiality.
- (iii) Securely place unneeded working documents or copies of confidential information in designated bins or shred them using cross-cut shredders for optimal security.
- (iv) For highly confidential documents, extra measures such as engaging certified document destruction services may be warranted.
- (v) Documents devoid of confidential content may be suitably recycled.
- (vi) Prior to disposing of any electronic media, including computers, hard drives, USB keys, etc., Employees must ensure these devices are properly formatted.
- (vii) Merely deleting a file does not completely erase it from a storage device. Employees should use secure file deletion software that overwrites the data, making it irretrievable.
- (viii) If external data destruction services are engaged, it is crucial to ensure they adhere to the organisation's security standards and provide a certificate of destruction upon completion.



5.10. Incident reporting and management

- a) Privacy incidents, such as unauthorised access, alteration, or destruction of personal information, can arise from human error, technical issues, or intentional actions, affecting both electronic and hard-copy data. These incidents must be promptly reported to minimise their impact.
- b) Any privacy incident, whether major or minor, or even a near miss with no apparent Participant impact, must be reported to the Incident Manager or other Key Personnel following the Incident Reporting Procedure.
- c) Employees should be proficient in recognising potential privacy incidents and must promptly report all incidents. The emphasis of reporting is not to penalise individuals, but to reduce the potential impact of the incidents.
- d) Defuse Behaviour Solutions is committed to notifying relevant authorities, such as the
 - 1) Department of Health and Human Services;
 - 2) NDIS Commission; and
 - 3) the Office of the Australian Information Commissioner,

within one business day upon recognising a potential privacy incident or receiving an allegation of a possible breach.

5.11. Training

- a) All Employees must undergo regular training to ensure they understand and comply with the Privacy and Information Management Policy and its associated procedures. Training will be provided upon induction and at regular intervals, as needed, or when procedures change.
- b) All Employees must adhere to these procedures to protect the rights and safety of our Participants.

6. Policy review and updates

This Policy will be amended and updated to comply with applicable laws and Regulations.

Approval Authority: Esme Jorgensen

Version: 1

Approval Date: July 2026

Review Date: July 2028