PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

Version 2.0: June 2026

PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

Purpose and Scope

This policy and procedure sets out staff responsibilities relating to collecting, using, protecting and releasing personal information, in compliance with privacy legislation. It applies to all:

- Bilingual Care staff
- aspects of Bilingual Care's operations and
- staff and consumer personal information.

This policy and procedure should be read in conjunction with Bilingual Care's *Records and Information Management Policy and Procedure*. It meets relevant legislation, regulations, and Standards.

Applicable Strengthened Aged Care Quality Standards

- Standard 1: The Person
- Standard 2: The Organisation
- Standard 3: The Care and Services
- Standard 5: Clinical Care

Consumers' privacy and confidentiality must be upheld at all times, in all aspects of service delivery and organisational management.

Interaction of Applicable Legislation and Associated Definitions

National Requirements

Aged Care Act 2024 (Cth) – regulates how personal information about Support at Home participants is handled by the Aged Care Quality and Safety Commission. This limits how the Commission collects and uses personal information and when and to whom information can be disclosed. The Commission must also comply with the *Privacy Act 1988 (Cth)*.

Privacy Act 1988 (Cth) - regulates how personal information about individuals is handled. The Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights, and obligations for the handling, holding, use, accessing and correction of personal information. The Act protects the privacy of an individual's information where it relates to Commonwealth agencies and private businesses (including not-for-profit organisations) with a turnover of more than $3 million. **All** organisations that provide a health service and hold health information (other than in a staff record) are covered by the Act.

Health Information – personal information or an opinion about:

- the health, including an illness, disability or injury, (at any time) of an individual
- an individual's expressed wishes about the future provision of health services to the individual or

- a health service provided, or to be provided, to an individual

that is also:

- Personal Information
- Other Personal Information collected to provide, or in providing, a health service to an individual
- Other Personal Information collected in connection with the donation, or intended donation, by an individual of his or her 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.

Informed consent: permission that is given after receiving information that is understood about the collection, use, storage, and disclosure of personal information.

Personal Information – information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not and
- whether the information or opinion is recorded in a material form or not.

Sensitive Information – personal information or an opinion 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
- criminal record

that is also:

- Personal Information
- Health Information about an individual
- genetic information about an individual 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.

Protected Information – information:

- about a person that is or was held in the records of the Agency or
- to the effect that there is no information about a person held in the records of the Agency.

New South Wales

Privacy and Personal Information Protection Act 1998 (NSW) – regulates how personal information is handled by NSW public sector agencies including government agencies, local councils, State Owned Corporations, and universities.

Personal Information - information or an opinion (including information or an opinion forming part of a database and whether recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics. It does not include any of the following:

- information about an individual who has been dead for more than 30 years
- information about an individual that is contained in a publicly available publication
- information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act
- information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth
- information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 1994*, or that has been collected in the course of an investigation arising out of a public interest disclosure

- information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*
- information about an individual arising out of a Royal Commission or Special Commission of Inquiry
- information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990*
- information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*
- information or an opinion about an individual's suitability for appointment or employment as a public sector official
- information about an individual that is obtained about an individual under Chapter 8 (Adoption information) of the *Adoption Act 2000*
- information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations.

Health Records and Information Privacy Act 2002 (NSW) – regulates how health information is handled by NSW public sector agencies, public sector health organisations, private sector organisations, health service providers and businesses with a turnover of more than $3 million which hold health information.

Health information –

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

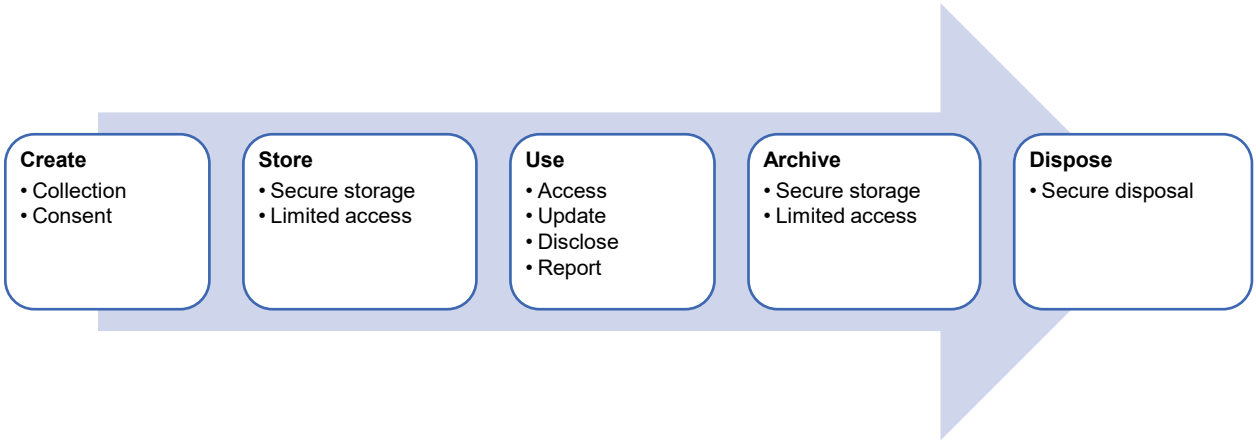
Private sector service providers in NSW must comply with the ***Privacy Act 1988 (Cth)*** and ***Health Records and Information Privacy Act 2002 (NSW)*** when handling health information. The ***NSW Information and Privacy Commission*** administers the HRIP Act and accepts complaints about health information.

Policy

Bilingual Care recognises, respects, and protects everyone's right to privacy, including the privacy of its consumers and staff. All individuals (or their legal representatives) have the right to decide who has access to their personal information.

Bilingual Care's privacy and confidentiality practices support and are supported by its records and information management processes (see the *Records and Information Management Policy and Procedure*).

Privacy and Confidentiality processes interact with the information lifecycle in the following ways:



All staff are responsible for maintaining the privacy and confidentiality of consumers, other staff and Bilingual Care.

Procedures

Roles and Responsibilities

The **Leadership Team** is responsible for:

- ensuring compliance with privacy and confidentiality obligations under the Aged Care Act 2024 (Cth), Aged Care Rules and applicable privacy legislation
- establishing and maintaining secure and effective systems for managing personal and health information, including storing, accessing and transmitting personal and health information
- ensuring privacy risks are identified, managed and reviewed as part of the organisation's risk management framework
- implementing safeguards to prevent unauthorised access, loss or misuse of information
- ensuring adequate resources, systems and workforce capability are in place to protect consumer information
- Bilingual Care's data breach response is documented in *Business Continuity Plan* and is accessible to staff
- overseeing responses to serious or systemic privacy breaches and assisting in investigations and responses to privacy incidents
- ensuring reporting obligations are met, including where incidents are notifiable to regulators, such as data breaches

The **Privacy Officer** is responsible for:

- providing advice and guidance on privacy and confidentiality obligations
- managing and coordinating responses to privacy breaches, complaints and requests for access or correction
- maintaining accurate and current records relating to consent, disclosure, complaints and breaches
- reporting to and liaising with regulators where required
- supporting data retention, archiving and disposal in line with legislative requirements
- ensuring all staff understand and comply with privacy and confidentiality requirements

Clinical and Allied Health Professionals are responsible for:

- collecting, using and disclosing personal and health information lawfully, ethically and on a need-to-know basis relevant to their scope of practice
- ensuring informed consent is obtained and documented for the use and sharing of information, including photos and videos
- maintaining accurate, secure and confidential records
- promptly reporting any actual or suspected privacy breaches
- supporting consumer choice, dignity and autonomy in all information-handling practices

Associated Providers and **Volunteers** are responsible for:

- complying with this policy and procedure, and all privacy and confidentiality requirements applicable to their role
- only accessing information authorised for their duties
- maintaining confidentiality during and after their engagement with Bilingual Care
- promptly raising privacy concerns and reporting actual or potential breaches of privacy in accordance with this policy and procedure

All **staff** are responsible for:

- upholding privacy and confidentiality as a core aspect of quality, safe and respectful care
- only accessing, using or sharing information that is required to perform their role
- ensuring that when collecting, storing, using, or disposing of personal and health information, including photos, videos, and other recordings, that they comply with the requirements of this policy and procedure
- respecting people's choices about being photographed or videoed and that images or recordings of people are used appropriately
- being aware of cultural sensitivities and the need for some images/recordings to be treated with special care,
- supporting consumers to raise concerns or complaints about privacy safely, and
- reporting suspected or actual privacy breaches in accordance with this policy and procedure, and Bilingual Care's *Incident Management policies and procedures*.

General

Bilingual Care's Privacy Officer is its Managing Director. The Privacy Officer is responsible for ensuring Bilingual Care complies with the requirements of the *Privacy Act 1988 (Cth)* as well as Aged Care Act 2024 (Cth). This includes developing, implementing, and reviewing processes that address:

- why and how Bilingual Care collects, uses and discloses personal information
- what information Bilingual Care collects about individuals and its source
- who has access to the information
- information collection, storage, access, use, disclosure, and disposal risks

- how individuals can consent to personal information being collected, withdraw, or change their consent and change information about them held by Bilingual Care
- how Bilingual Care safeguards and manages personal information, including how it manages privacy queries and complaints and
- how information that needs to be updated, destroyed, or erased is managed.

The Privacy Officer reviews these processes regularly, through annual Privacy Audits (see Bilingual Care's *Privacy Audit Form* and *Schedule 2. Internal Review and External Audit Checklist)*.

All staff are responsible for complying with this policy and procedure and their privacy, confidentiality, and information management obligations. Staff must keep personal information about consumers, other staff, and other stakeholders confidential, in accordance with the confidentiality provisions in their employment contract.

As per Bilingual Care's *Onboarding and Induction Policy and Procedure*, all staff must undergo Induction, which includes training in privacy, confidentiality, and information management. Staff knowledge and application of confidentiality, privacy and information management processes is monitored on a day-to-day basis and through annual Performance Reviews. Additional formal and on-the-job training is provided to staff where required.

Bilingual Care's *Privacy Statement* must be prominently displayed in Bilingual Care's premises and included in Bilingual Care's *Consumer Information Pack.*

The *Privacy Statement* and a full copy of this policy and procedure must be provided upon request.

Information Collection and Consent

Consumer Information Collection and Consent

Bilingual Care will only request personal information that is necessary to:

- assess a potential consumer's eligibility for a service
- provide a safe and responsive service
- monitor the services provided and
- fulfil government requirements for non-identifying and statistical information.

Personal consumer information that Bilingual Care collects includes, but is not limited to:

- contact details for consumers and their representatives/carers
- details for emergency contacts and people authorised to act on behalf consumers
- consumers' health status and medical records
- medication records (if appropriate)
- service delivery intake, assessment, monitoring, and review information
- assessments, reviews, and service delivery records
- external agency information
- feedback and complaints
- incident reports and
- consent forms.

Prior to collecting personal information from consumers or their representatives, staff must explain:

- that Bilingual Care only collects personal information that is necessary for safe and effective service delivery

- that personal information is only used for the purpose it is collected and is stored securely
- what information is required
- why the information is being collected and how it will be stored and used
- the occasions when the information may need to be shared and who or where the information may be disclosed to
- the consumer's right to decline providing information
- the consumer's rights in terms of providing, accessing, updating, and using personal information, and giving and withdrawing their consent and
- the consequences (if any) if all or part of the information required is not provided.

Consumers and their representatives must be provided with Bilingual Care's *Privacy Statement* and informed that a copy of this policy and procedure is available on request.

Staff must provide privacy information to consumers and/or their family and supporters in ways that suit their individual communication needs. Written information can be provided in different languages and Easy English or explained verbally by staff. Staff can also help consumers access interpreters or advocates where required.

After providing the above information, staff must use a *Consent Form* to:
- confirm the above information has been provided and explained and
- obtain consent from consumers or their legal representatives to collect, store, access, use, disclose and dispose of their personal information.

Consumers and their representatives are responsible for:
- providing accurate information when requested
- completing *Consent Forms* and returning them in a timely manner
- being sensitive and respectful to people who do not want to be photographed or videoed and
- being sensitive and respectful of the privacy of other people in photographs and videos when using and disposing of them.

Aged Care Audits

Consumers who do not wish to participate in audit interviews have the right to decline. They may also choose not to participate in discussions with auditors or have their care observed during an audit. Their decision will be respected by Bilingual Care and will be documented in their consumer file in Ezihealth.

Collection and Use of Photos and Videos

Photos, videos, and other recordings are a form of personal information. This includes photos and videos taken for the purpose of service delivery and other purposes such as marketing and promotions.

Photos and videos of consumers must only be collected, used or shared where there is a clear care-related or organisational purpose and informed consent has been obtained in advance. Consent must be sought in a way that is accessible and appropriate to the consumer's capacity, with the involvement of their family/supporters where required.

Bilingual Care will obtain informed consent from the consumer using the *Social Media Consent Form*. Staff must clearly explain to the consumer:
- the purpose for collecting the photo or video (e.g. care planning, clinical review, training, quality improvement or communications)

- how and where the image or recording will be used or published, including whether it may appear in:
  - internal systems or records
  - staff training materials
  - organisational publications
  - websites, newsletters or social media platforms
- who may have access to the photo or video
- how long the photo or video will be retained
- that consent is voluntary, may be withdrawn at any time, and that withdrawal of consent will not impact the delivery of their care.

Photos and videos must not be used for any purpose outside the scope of the consent provided, and additional consent must be obtained if the proposed use changes.

All consents must be documented and stored securely, and photos or videos must be managed in accordance with privacy, confidentiality and record-keeping requirements. Where consent is not provided, or is withdrawn, photos or videos must not be collected or must be deleted or de-identified as appropriate.

Cultural Considerations

In addition to obtaining informed consent, special care must be taken when collecting, using or sharing photos or videos where cultural beliefs, practices or sensitivities may apply. For Aboriginal and Torres Strait Islander peoples, images, names or recordings of a person who has passed away, or the sharing of certain visual or audio materials, may cause significant cultural distress. Cultural protocols, community preferences and guidance from the consumer, their family/supporters or community representatives must be respected at all times.

Where a consumer identifies specific cultural, religious or spiritual sensitivities, including restrictions on photography, filming, storytelling or publication, these requirements must be documented on the *Social Media Consent Form* and strictly adhered to. Photos or videos must not be used, published or retained in a way that is inconsistent with cultural practices, even where general consent may have been given.

Staff Information Collection and Consent

Personal staff information that Bilingual Care collects includes, but is not limited to:

- tax declaration forms
- superannuation details
- payroll details
- employment contracts (where applicable)
- personal details
- emergency contact details
- medical details (if appropriate)
- Police Checks / Worker Screening Checks
- qualifications
- First Aid, CPR, Anaphylaxis, and other relevant certificates and
- personal resumes.

Where relevant, forms used to collect the above information will also obtain staff members' consent to collect, store, access, use, disclose and dispose of their personal information.

Storage

Refer to the *Records and Information Management Policy and Procedure* for details on how Bilingual Care securely stores and protects staff and consumer personal information.

Access

Staff personal information must only be accessed by the Managing Director, who may only access the information if it is required to perform their duties.

Staff must only access consumers' personal information if it is required to perform their duties.

Staff and consumers have the right to:

- request access to personal information Bilingual Care holds about them, without providing a reason for requesting access
- access this information and
- make corrections if they believe the information is not accurate, complete, or up to date.

All **consumer** access or correction requests must be directed to the Managing Director.

All **staff** access or correction requests must be directed to the Managing Director.

Within 2 working days of receiving an access or correction request, the responding staff member will:

- provide access, or explain the reasons for access being denied
- correct the personal information, or provide reasons for not correcting it or
- provide reasons for any anticipated delay in responding to the request.

An access or correction request may be denied in part or in whole where:

- the request is frivolous or vexatious
- it would have an unreasonable impact on the privacy of other individuals
- it would pose a serious threat to the life or health of any person or
- it would prejudice any investigations being undertaken by Bilingual Care or any investigations it may be the subject of.

Any consumer access or correction requests that are denied must be approved by the Privacy Officer and documented on the consumer's file.

Any staff access or correction requests that are denied must be approved by the Privacy Officer and documented on the staff member's file.

Information Sharing and Disclosure

A consumer's personal or health information may be shared if:

- the consumer (or their authorised representative) has provided informed consent
- information sharing is required for:
  - delivery or coordination of care
  - clinical decision-making
  - risk management or safeguarding
- disclosure is required or authorised by law, including:
  - mandatory reporting obligations
  - Serious Incident Response Scheme (SIRS)

- regulator requests
- sharing is necessary to prevent serious harm to the consumer or others

Any limitations or conditions placed on consent must be recorded and respected.

Before sharing information, staff must consider:
- cultural, religious or spiritual sensitivities
- preferences of Aboriginal and Torres Strait Islander consumers
- any documented restrictions on information sharing

Information must not be shared in a way that causes unnecessary distress or breaches cultural protocols unless there is a legal or safety requirement to do so.

Disclosure Without Consent

Consumer or staff personal information may only be disclosed:
- for emergency medical treatment
- to outside agencies with the person's permission
- with written consent from someone with lawful authority or
- when required by law, or to fulfil legislative obligations such as mandatory reporting.

If a staff member is in a situation where they believe that they need to disclose information about a consumer or other staff member that they ordinarily would not disclose, they must consult the Privacy Officer before making the disclosure.

International Disclosure

Under the *Privacy Act 1988*, before Bilingual Care discloses personal information to an overseas recipient, it must take reasonable steps to ensure the overseas recipient does not breach Principle 8 of the Australian Privacy Principles (APPs).

The Privacy Officer is responsible for undertaking these investigations.

This requirement does not apply if:
- the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially like protection given under the APPs, and
- there are mechanisms available to enforce that protection.

Reporting

Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) Scheme is a national scheme that operates under the *Privacy Act 1988 (Cth)*. requires organisations to report certain data breaches to people impacted by the breach, as well as the Australian Information Commissioner.

A data breach occurs when personal information about others is lost or subject to unauthorised access. A data breach may be caused by malicious action, human error or a failure in information management or security systems.

In addition to harm caused to people who are the subject of data breaches, an incident like this may also cause Bilingual Care reputational and financial damage.

Further detail about the NDB Scheme is contained on the Office of the Australian Information Commissioner (OAIC)'s website.[1]

Bilingual Care's *Data Breach Response Plan* outlines its strategy for containing, assessing, and managing data breach incidents.

Notifiable Data Breaches

A Notifiable Data Breach, also called an 'eligible data breach', occurs when:

- there is unauthorised access to or disclosure of personal information, or information is lost in circumstances where unauthorised access or disclosure is likely to occur
- the disclosure or loss is likely to result in serious harm to any of the people that the information relates to. In the context of a data breach, serious harm may include serious physical, psychological, emotional, financial, or reputational harm and
- Bilingual Care has been unable to prevent the likely risk of serious harm through remedial action.

If Bilingual Care acts quickly to remediate a data breach and as a result it is not likely to result in serious harm, it is not considered a Notifiable Data Breach.
See Bilingual Care's *Business Continuity Plan*, for response actions.

Detecting Data Breaches

Examples of data breaches include:

- loss or theft of devices (such as phones, laptops, and storage devices) or paper records that contain personal information
- unauthorised access to personal information by a staff member, for instance, a staff member browsing sensitive consumer records without a legitimate purpose or a computer network being compromised by an external attacker resulting in personal information being accessed without authority
- unauthorised disclosure of personal information due to 'human error', for example an email sent to the wrong person and
- disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures.

In reality, and particularly with respect to electronic data, data breaches can be difficult to detect. As such, all staff are responsible for:

- adhering to all Bilingual Care Policies, Procedures and processes relating to data creation, storage, use, archiving and disposal
- only transporting hard copy files and electronic storage devices in a secure, lockable container and with approval from the Managing Director
- implementing password protection and two-factor or multi-factor authentication on devices and software used to access Bilingual Care information
- ensuring all operating systems, browsers and plugins used on devices to access Bilingual Care information are up to date with patches and fixes and have appropriate security maintenance software installed and active and
- completely shutting down devices used to access Bilingual Care information at least once a week, to ensure updates are installed.

[1] Office of the Australian Information Commissioner 2024, *Data Breach Preparation and Response*, Australian Government, accessed 20 April 2026, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response

The Managing Director is responsible for ensuring that:

- security maintenance software is installed on all Bilingual Care computers, to detect breaches as well as any peculiar activity
- all operating systems, browsers and plugins used on Bilingual Care devices are up to date with patches and fixes
- software systems used by staff lock users out after multiple failed login attempts
- they are listed as a key contact person for notification from third party software providers in the event those systems are breached and
- they are subscribed to a data breach notification service so they are kept abreast of possible data breaches that could impact Bilingual Care.

The Leadership Team is responsible for ensuring that:

- annual Privacy Audits are undertaken in accordance with *Schedule 2. Internal Review and External Audit Checklist* and
- all staff are adequately and regularly trained in all Bilingual Care Policies, Procedures and processes relating to data creation, storage, use, archiving and disposal.

Reporting a Data Breach

All staff must report all potential or actual data breaches (including unusual activity in electronic systems and loss or theft of files or storage devices) as soon as possible to the Privacy Officer, who will determine Bilingual Care's response and whether the breach needs to be reported under the NDB Scheme.

Responding to a Data Breach

If the Privacy Officer suspects that a data breach is notifiable under the NDB Scheme, they must make an assessment to determine if this is the case.

If the Privacy Officer believes that the data breach is notifiable under the NDB Scheme, they must notify Bilingual Care's Data Breach Response Team. This team comprises the:

- Managing Director as Team Leader, responsible for leading the response team and reporting to the Leadership Team
- Managing Director as Project Manager, to coordinate the team and provide support to its members
- Privacy Officer, to bring privacy expertise to the team
- Managing Director as legal support, to identify legal obligations and provide advice
- Managing Director as risk management support, to assess the risks from the breach
- Managing Director as Information and Communication Technology (ICT) or forensics support, to help establish the cause and impact of a data breach that involves ICT systems
- Managing Director to provide information and records management expertise, assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and provide advice on recording the response to the data breach
- Managing Director as Human Resources support, if the breach was due to the actions of a staff member and
- Managing Director to provide media/communications expertise and assist in communicating with affected individuals and dealing with the media and external stakeholders.

The Data Breach Response Team must notify all impacted individuals of the breach as soon as is practicable.

All data breach incidents (whether notifiable or not) must be responded to in accordance with Bilingual Care's *Business Continuity Plan* and recorded in Bilingual Care's *Incident Register*, with relevant actions tracked in its *Continuous Improvement Plan* where appropriate.

Where a breach is referred to the Data Breach Response Team, its response will be based on the following steps:

- **Step 1:** Contain the data breach
- **Step 2:** Assess the data breach and the associated risks
- **Step 3:** Notify individuals, the Australian Information Commissioner and Aged Care Quality and Safety Commission
- **Step 4:** Prevent future breaches.

See Bilingual Care's *Business Continuity Plan* for further detail.

Notifiable Data Breaches Involving More Than One Entity

The NDB Scheme recognises that personal information is often held jointly by more than one entity. For example, one entity may have physical possession of the information, while another has legal control or ownership of it. Examples include:

- where information is held by a cloud service provider
- subcontracting or brokering arrangements and
- joint ventures.

In these circumstances, an eligible data breach is considered the responsibility of both entities under the NDB Scheme. However, only one entity needs to take the steps required by the NDB Scheme and this should be the entity with the most direct relationship with the people affected by the data breach. Where obligations under the Scheme (such as assessment or notification) are not carried out, both entities will be in breach of the Scheme's requirements.

Other Reporting Requirements

The Privacy Officer must immediately notify the Aged Care Quality and Safety Commission and if they become aware of a breach or possible breach of privacy legislation.

Data Breach Reporting under SIRS

A data breach may constitute a reportable incident under the Serious Incident Response Scheme (SIRS) where it has resulted in, or is reasonably likely to result in, harm or distress to a consumer. This may include unauthorised access to, disclosure of, or loss of personal or health information that compromises a consumer's privacy, dignity, safety or wellbeing.

If a data breach meets the threshold of a reportable incident, the Privacy Officer must notify the Aged Care Quality and Safety Commission within the required SIRS timeframes, in addition to managing the breach in accordance with privacy legislation and internal incident management procedures. See Bilingual Care's *Consumer Incident Management Policy and Procedure* for SIRS reporting guidelines.

Data breaches may also trigger reporting obligations outside of the *Privacy Act 1988*, such as to:

- Bilingual Care's financial services provider
- police or other law enforcement bodies
- the Australian Securities and Investments Commission (ASIC)

- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the Australian Cyber Security Centre (ACSC)
- the Australian Digital Health Agency (ADHA)
- Federal, State or Territory Government departments
- professional associations and regulatory bodies and
- insurance providers.

To support Bilingual Care's compliance with the Standards, the Privacy Officer will:

- review the Australian Cyber Security Centre's (ACSC) Information Security Manual (ISM)[2] and implement relevant principals and guidelines,
- implement the ACSC's Essential Eight,[3] which are eight essential mitigation strategies to help protect against cyber threats, and
- subscribe to ACSC Alerts,[4] to obtain information on threats and how to keep information assets secure online.

Archiving and Disposal

Refer to the *Records and Information Management Policy and Procedure* for details on how Bilingual Care archives and disposes of consumers' personal information.

Supporting Documents

Documents relevant to this policy and procedure include:

- *Records and Information Management Policy and Procedure*
- *Onboarding and Induction Policy and Procedure*
- *Schedule 2. Internal Review and External Audit Checklist*
- *Business Continuity Plan*
- *Data Breach Response Plan*
- *Privacy Audit Form*
- *Privacy Statement*
- *Consumer Information Pack*
- *Incident Register*
- *Consent Form*

Monitoring and Review

This Policy and Procedure will be reviewed at least every two years by the Leadership Team. Reviews will incorporate staff, consumer, and other stakeholder feedback.

[2] Australian Cyber Security Centre, 2026, *Information Security Manual (ISM)*, ACSC, Australian Signals Directorate (ASD), Australian Government, accessed 20 April 2026, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

[3] Australian Cyber Security Centre, 2026, *Essential Eight*, ACSC, Australian Signals Directorate (ASD), Australian Government, accessed 20 April 2026, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

[4] Australian Cyber Security Centre, 2024, *Homepage*, ACSC, Australian Signals Directorate (ASD), Australian Government, accessed 20 April 2026 https://www.cyber.gov.au/.

Bilingual Care's feedback collection mechanisms, such as staff and consumer satisfaction surveys, will assess:

- satisfaction with Bilingual Care's privacy and confidentiality processes
- whether stakeholders have received adequate information about privacy and confidentiality and
- the extent to which consumers and their supporters feel their privacy and confidentiality has been protected.

Bilingual Care's *Continuous Improvement Plan* will be used to record improvements identified and monitor the progress of their implementation. Where relevant, this information will be considered as part of Bilingual Care's service planning and delivery processes.

DOCUMENT CONTROL

Version No.	Issue Date	Document Owner
2.0	26/06/2026	MD
Version History		
Version No.	**Reviewed Date**	**Revision Description**