Privacy Policy

1.0 Implementation of Australian Privacy Principles

APP 1- Open and transparent management of personal information

Management are to ensure that referrers have obtained Participant consent prior to making a referral to YBSS. This may be verbal or in writing.

During intake processes employees of YBSS are to check with the participant that they have consented to the referral to our service. The participant is to be informed about what information will be gathered about them during the assessment process and how that information will be utilised and stored.

During employee and Board member onboarding Management will ensure that all personnel are provided with induction on YBSS' approach to the Management of information.

Informing the person from whom information is collected

Employees will clarify with the participant and/or their nominated person the accuracy of information received through the referral process and will make them aware:

- that information is being collected and for which purposes
- of the intended recipients of the information
- whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided
- of the participant's right of access to, and correction of the information
- how records are kept – i.e participant paper file and electronic database
- That the participant has the right to withhold information for privacy reasons.

The only information held by the organisation about a participant will be information necessary to assess the need for a service, and to provide the service. Information will be as objective as possible, yet relevant and up-to-date.

APP 2-Anonymity and pseudonymity

YBSS are required to identify Participants receiving services to funding bodies. It is therefore unlawful and impractical for us to deal with Participants who have not identified themselves.

APP3 – Collection of solicited personal information

Personal information is collected by YBSS for the primary purposes of appropriate quality service provision in a safe and healthy environment to meet individual requirements, to meet duty of care obligations, and initiate appropriate referrals and coordination of supports. Due to the nature of operations, the organisation is

unable to provide participant anonymity; however, at all times participant privacy and confidentiality is respected.

YBSS collects and maintains personal information that includes:

Role	What we collect	Purpose for collection
Participant	• Advocate • Guardian / Financial Administrator • Relationship Networks • Safety and Behaviours • Abilities and Daily Living Skills • Communication • Health and Medication related information • NDIA Plan • Service budget • Service agreement • Services received • Interests and goals and photographs and video of progress toward goals • Approved funding arrangements with government bodies and other agencies • Government entitlements • Relevant stakeholder relationships such as allied health providers, LAC and mainstream supports • Reports and information from stakeholders • Referrals • Accommodation and living arrangements • Consent forms • Aides and equipment information • Complaints • Participant progress notes • Participant Risk Assessments • Participants Incident Reports	• Prioritising and processing referrals and the coordination of supports; • Assessing Participants service needs and offering service to meet those needs • Providing relevant agreed services to Participants • Assessing WHS status of participant's homes for the purpose of service provision • Service provision • Appropriate training and development of personnel • Communication within the team of personnel regarding participant's success, activities and progress toward goals • Continuity of care • Keeping participant records • Sending out and processing participant accounts and Payment requests • Meeting funding, legal and regulatory requirements • Quality measurement and management. • Reporting on participant where required, provide this to external bodies • Disaster Management • For the purposes of NDIS Quality Audit verification
Participant's nominated person	• Name • Date of birth • Address • Contact details • Religion, culture, and language • Living arrangements • Carer needs and quality of life	• Emergency contact for participant • Service planning and review • Quality Management and measurement • For the purposes of NDIS Quality Audit verification • Disaster Management

Employees or volunteers	• Name • Date of birth • Address • Contact details • Next of kin contact details • Country of birth, citizenship status, residency or visa status • Details of previous employment • Qualifications, skills and experience • Information obtained in referee checks • Criminal History screening records • Drivers Licence details • Performance records such as supervision, peer review and appraisals • Grievance or complaints records • Training and Professional development records • Resignation or termination of employment records • The terms and conditions of employment – employment Contract • Personal details relevant to payroll processes such as pay rates, hours of work, bank details, Tax file number, leave entitlements, payroll deductions and superannuation • Secondary Place of employment • Incident Reports • Photos and Video • Signed agreements such as Code of Conduct and Ethics, Confidentiality, Contract of Employment and Policy acknowledgement • Vaccination Status Certificates (Flu and COVID)	• To deliver YBSS services • Recruitment, selection and appointment functions to become a volunteer or employee of our organisation • To facilitate a placement in an appropriate service or position • To assist with services whilst an individual is employed or engaged as a volunteer with Yumba Bimbi Support Services • For the purposes of NDIS Quality Audit verification • Ongoing human resources management such as; • Superannuation administration • Workplace health, safety and workers compensation • Staff training and development • Staff appraisals, probation and promotion • To deal with management of grievances or disciplinary procedures • To meet legislative responsibilities to all volunteers and employees • To meet legislative and quality responsibilities to Participants • To obtain feedback from individuals about their experiences • To assist Yumba Bimbi Support Services to review and improve its programs and services developments and opportunities • For purposes required by legislation, for example Australian taxation legislation, employment legislation and immigration legislation • Payroll processing • For the recovery of debts • For insurance purposes • Other processes such as reporting on workforce profiles in an aggregate (non-identifying) format and, where required, provide this to external bodies • Verification of Vaccination status for flu and COVID 19 is required by law to manage rosters in providing disability

		accommodation or aged care services. • Verification of COVID 19 Vaccination status is required to ensure compliance with Federal Government reporting requirements. • Disaster Management
Donors, sponsors and business partners	• Contact details (name, address, telephone numbers, email etc.) • Donation history • ABN if required • Memorandums of Understanding areas of interest by category and industry • Bank details (if YBSS is to receive payment or make payment for services received) • Type of support (e.g. Workplace giving, goods in kind, program support, volunteering)	• Accounts payable and receivable • Acknowledgement and promotion of; • Fundraising activities • Special events and initiatives • Partnerships • Community Support • Corporate relationships • Accurate financial records and reporting • To comply with legal obligations • To provide transparency relating to donated funds, particularly for Appeals for public donations
Members	• Contact details (name, address, telephone, numbers, email etc) • Date of birth • Areas of interest	• To provide YBSS services • To provides communication updates and ensure transparency • Relating to donated funds, particularly appeals for public donations, and YBSS operations • To process donations and provides accurate receipts • To facilitate ongoing fundraising and marketing activities • To provide info about YBSS • To receive invitations to upcoming events and activities • To recognise the support of YBSS
Contractors	• Contact details (name, address, telephone, numbers, email etc) • Bank Details • COVID 19 Vaccination status for entry into Disability Accommodation Services	• To book servicing/appointments • Accounts payable and receivable • Compliance with Qld Health Directions
Board members	• Contact details (name, address, telephone numbers, email etc.)	• To provide good governance and leadership to YBSS

	• Date of birth • Qualifications and educational background • Work history and skills sets • Board representation history ○ Vested interests which may cause conflict in board role.	• To facilitate the activities of YBSS • Ensure transparency in the activities of YBSS • To provide communication updates • To receive and disseminate information pertaining to the activities of YBSS.

APP 4- Dealing with unsolicited personal information

YBSS will advise participants, employees, volunteers, or members of any information obtained or collected, including unsolicited personal or sensitive information. If the information received is not relevant to the role within YBSS, function and activities YBSS will either destroy the information or deidentify the information.

APP 5- Notification of the collection of personal information

All YBSS participants, employees, volunteers, or members will be advised during Intake and Assessment, recruitment or appointment processes about what information YBSS collects and for what purpose.

How we collect: We collect information through various means, including telephone and in-person interviews, appointments, forms and questionnaires. If a person feels that the information that we are requesting, either on forms or in discussions and meetings, is not information that they wish to provide, they are encouraged to raise this with us.

In some situations we may also obtain personal information about people from a third party source. When we collect information in this way, we will take reasonable steps to contact the relevant person and ensure that they are aware of the purposes for which we are collecting personal information and the organisations to which we may disclose their information, subject to any exceptions under the Act.

Sources of information

We obtain personal information from the following:

- the individual to whom the information relates
- the parent or guardian if a person is under the age of 16 years or has an official guardian who is authorised to pass on such information
- other persons or mainstream services whom the individual has authorised to pass on the information
- other health or service providers whom the individual has authorised to pass on information to YBSS
- government agencies or funding bodies such as the NDIA or disability services
- previous employers whom the individual has authorised to pass on information to YBSS.

Withdrawing consent

A person may withdraw or change consent release of information at any time by contacting either YBSS management (for participants, employees and volunteers) or the YBSS Executive Assistant for member related issues.

APP 6- Use or disclosure of personal information

The organisation does not disclose any of the above information to others without

consent from the individual. On intake, participants wanting to access the organisation's services will be requested to sign a consent form which includes consent to share personal information in particular circumstances – responding to disaster and emergency services, funding bodies, regulators, authorisation to obtain medical information, on the YBSS website and social media platforms, staff professional development and case management, communication and information regarding a participant's progress toward goals and achievements.

YBSS does not disclose or release information to any persons or entities outside of Australia without the express knowledge and consent of the participant or their nominated person.

YBSS releases or discloses personal information only as permitted as required under Australian legislation i.e. mandatory reporting, reporting as per government funding contracts.

YBSS will not disclose an individual's personal information to a third party unless one of the following applies:

- the individual has consented
- the individual would reasonably expect us to use or give that information for another purpose related to the purpose for which it was collected (or in the case of sensitive information—directly related to the purpose for which it was collected)
- it is otherwise required or authorised by law
- it will prevent or lessen a serious threat to somebody's life, health or safety or to public health or safety
- it is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities
- it is reasonably necessary to assist in locating a missing person
- it is reasonably necessary to establish, exercise or defend a claim at law
- it is reasonably necessary for a confidential dispute resolution process
- it is necessary to provide a health service
- it is necessary for the management, funding or monitoring of a health service relevant to public health or public safety.
- It is reasonably necessary for the enforcement of a law conducted by an enforcement body.

APP 7- Direct marketing

In the instance where a person consents in writing, the collection of personal information for the purposes of marketing may occur.

YBSS publishes newsletters quarterly—these publications may contain employee, participant or Board images or information but only with the express written consent of the person or their nominated person.

YBSS utilises mainstream media and social media for the purposes of marketing, communication and education. Personal information may only be used with the express written consent of the person or their nominated person.

All people are free to refuse consent for personal information to be utilised in marketing or to receive marketing material.

YBSS does not use cookies within its website www.yumbabimbi.com.au to track user traffic, geographical location or other.

APP 8- Cross border disclosure of personal information

As per APP 6 above.

APP 9 – Adoption, use or disclosure of government related identifiers

YBSS may use government related identifiers for the purposes of reporting to government only as per funding contracts and legislation.

APP 10- Quality of personal information

YBSS will ensure that all information collected and retained by the organisation in relation to participants, employees, volunteers and members is accurate, up to date and complete. On an annual basis, Participants and personnel will be required to review their personal details and consent forms to ensure currency.

APP 11- Security of personal information

YBSS ensures that it provides security and protection of personal information from misuse, interference and loss and unauthorised access, modification or disclosure. We protect the personal information we hold by maintaining physical, electronic and procedural safeguards.

Protecting personal Information

The organisations physical safeguards include:

- an individual file is created for each participant and personnel following initial assessment or interview
- participant and personnel files are stored in the organisation's central filing systems on Supportability and Employment Hero and Boardwise. Each platform is password protected and has a structured level of permission and security relating to access of information
- Hard copy files of the participant and personnel information are locked at the end of each working day
- ensuring participant and personnel information is up to date at all times
- employees maintain a 'clear desk' policy—this means that all participant and personnel files in addition to financial and other information sensitive to the operations of YBSS are filed in their appropriate place in the locked filing drawers and all software systems and platforms are logged out of at the end of each working day
- staff utilising tools or data management systems as adopted by the organisation.
- YBSS employs computer and network security data management measures
- software systems and data storage are classed strictly as 'on shore' and based only in Australia
- access to participant and personnel information is limited to authorised staff depending on classification and functions of role.

The organisation's procedural safeguards include:

- all employees and board are trained in confidentiality and the Privacy Act
- all employees have a signed confidentiality agreement acknowledging their commitment to the obligations and responsibilities as outlined in the policy
- contractors or people working on site, are required to sign a confidentiality agreement
- if an outside person enters the office, the staff member closes the computer screen if it shows personal Participant and personnel information
- meetings with visitors take place in organisation's meeting rooms whenever possible
- meetings with participants and personnel are only be conducted in an area which allows sufficient privacy.

APP 12-Access to personal information

Access to own information

Under the Australian Privacy Principles Participants employees, volunteers or Board members have the right to access their own information held by the organisation. If an individual requests access to the personal information we hold about them, or requests that we change that personal information, we not will allow access or make the changes unless we consider that there is a sound reason under the Privacy Act or other relevant law.

Participants and personnel can make a request to the Service Coordinator/s or General Manager or CEO verbally or in writing. Members can make a request to the Secretary of the organisation verbally or in writing.

The organisation will validate the identity of anyone making a request to access participant or personnel information. This is to ensure that information is not passed to a person who is not authorised to receive it.

For security reasons, people requesting information may be required to put their request in writing and provide proof of identity. This is necessary to ensure that personal information is provided only to the correct individuals and that the privacy of others is not undermined.

In the first instance, YBSS will generally provide a summary of the information held about the individual. It will be assumed (unless told otherwise) that the request relates to current records. These current records will include personal information which is included in YBSS databases and in paper files, and which may be used on a day to day basis.

YBSS will provide access by allowing the individual to inspect, take notes or print outs of personal information that we hold about them. If personal information (for example, name and address and contact details) is duplicated across different databases, YBSS will generally provide one printout of this information, rather than multiple printouts.

YBSS will take all reasonable steps to provide access or the information requested within 14 days of the request. In situations where the request is complicated or requires access to a large volume of information, YBSS will take all reasonable steps to provide access to the information requested within 30 days.
If an individual is able to establish that personal information YBSS holds about her/him is not accurate, complete or up to date, YBSS will take reasonable steps to correct our records.

Access will be denied if:

- the request does not relate to the personal information of the person making the request
- providing access would pose a serious threat to the life, health or safety of a person or to public health or public safety
- providing access would create an unreasonable impact on the privacy of others
- the request is frivolous and vexatious
- the request relates to existing or anticipated legal proceedings
- providing access would prejudice negotiations with the individual making the request
- access would be unlawful
- denial of access is authorised or required by law
- access would prejudice law enforcement activities
- access would prejudice an action in relation to suspected unlawful activity, or misconduct of a serious nature relating to the functions or activities of YBSS
- access discloses a 'commercially sensitive' decision making process or

information, or
- any other reason that is provided for in the APPs or in the Privacy Act.

If YBSS deny access to information wYBSS will set our reasons for denying access. Where there is a dispute about the right of access to information or forms of access, this will be dealt with in accordance with the complaints procedure set out below.

Inspection of Records - YBSS may be reviewed by the National Disability Insurance Agency or The NDIS Quality and Safeguards Commissions in relation to supports and services. The organisation will cooperate fully with the both agencies with respect to any review or audit.

As part of any review or audit, or as otherwise reasonably requested by the such regulatory bodies to carry out its rights and obligations under law, we must give those permitted personnel from such bodies access to premises where accounts and records associated with the provision of services to Participants are stored and allow those permitted to inspect and copy all records associated with the delivery of services to Participants.

APP 13- Correction of personal information

If Participants and personnel find that the personal information we hold on them is not correct, complete or up-to-date, the organisation will correct their records accordingly.

Length of time records are held

Participant and personnel records are archived and retained for 7 years, once the exit procedures have been completed.

The retention period for financial and payroll records is 7 financial years.

The retention period for all other records (Board, Governance and management, membership,) is 7 years from the date of the latest document on file.
Archiving is stored physically at a secured storage facility as well as archived electronically.

Archiving will be destroyed via an external third party shredding service as per the retention guidelines.

Complaints procedures

If a person whose personal or sensitive information has been collected by YBSS feels that the privilege of that information has been mismanaged a person has the right to make a complaint and have it investigated and dealt with under the YBSS Complaints procedure.

A person with a complaint about YBSS privacy practices or the handling of personal and sensitive information please contact the CEO of YBSS.
All complaints will be logged in the YBSS Complaints Register.

A privacy complaint relates to any concern that a person may have regarding YBSS privacy practices or the handling of personal and sensitive information. This could include matters such as how information is collected or stored, how information is used or disclosed or how access is provided to personal and sensitive information.

Effective investigation and resolution of a complaint within a reasonable timeframe usually within 10 working days should occur as soon as practicable.

However, in some cases, particularly if the matter is complex, the resolution may take longer.

Once the complaint has been made, YBSS will try to resolve the matter in a number

of ways such as:

- Request for further information: We may request further information from the complainant. The complainant should be prepared to provide YBSS with as much information as possible, including details of any relevant dates and documentation. This will enable YBSS to investigate the complaint and determine an appropriate solution. All details provided will be kept confidential.
- Discuss options: We will discuss options for resolution and make suggestions about how the matter might be resolved.
- Investigation: Where necessary, the complaint will be investigated. We will try to do so within a reasonable time frame. It may be necessary to contact others parties in order to proceed with the investigation. This may be necessary in order to progress a complaint.
- Conduct of YBSS employees, volunteers and Board members: If a complaint involves the conduct of an employee, volunteer or board member the matter will be raised with the person of concern in order to seek their comment and input in the resolution of the complaint.
- The complaint is substantiated: If a complaint is found to be substantiated, the complainant will be informed of the finding. YBSS will then take appropriate agreed steps to resolve the complaint, address, concerns and prevent the problem from recurring. A substantiated breach of privacy will result in disciplinary action for employees, volunteers and Board members.
- If the complaint is not substantiated, or cannot be resolved to the complainant's satisfaction, but this Privacy Policy has been followed, YBSS may decide to refer the issue to an appropriate intermediary. For example, this may mean an appropriately qualified lawyer or an agreed third party, to examine the investigation records and other documentation and/or act as a mediator.
- At the conclusion of the complaint, if the complainant is still not satisfied with the outcome the complainant is free to take the complaint to the Office of the Australian Information Commissioner or to the NDIS Quality and Safeguards Commission.

YBSS will keep a record of the complaint and the outcome in the Complaints Register.

YBSS are unable to deal with anonymous complaints. This is because we are unable to investigate and follow-up such complaints. However, in the event that an anonymous complaint is received we will note the issues raised and, where appropriate, try to investigate and resolve them appropriately.

2.0 Record Retention and Disposal

Type of record	Document description	Minimum time for retention	Form of retention	Disposal
Financial records including payroll		7 Financial years	If financial records are kept in electronic form, they must be converted into hard copy within a reasonable time. ATO accepts scanned copies.	Expunge from server and/or shred
Legal documents		10 years	Original records	Shred
Participant files and records		7 years from date of exit	Electronic or paper	De-identify personal information and

				expunge from computer or shred documents
Employment records		7 years from date of exit	Electronic or paper	De-identify personal information and expunge from computer or shred documents
Board/committee materials		7 years	Electronic or paper	Expunge from server and/or shred
Marketing and sales documents		5 years	Electronic or paper	Expunge from server and/or shred
Electronic mail		3 years	Electronic	Expunge from server

3.0 Data Breach

Data breaches are serious situations that have the potential to harm participants, workers and our organisation due to the leaking of sensitive information (such as personal identification numbers, health information and financial information).

Our organisation is committed to having robust mechanisms in place to prevent data breaches and we will establish a planned approach to address any real or suspected breaches of data.

To **prevent data breaches**, our organisation will:

- always respect the privacy and dignity of all participants
- ensure that all methods of data collection, both online and offline, have robust security measures in place
- verify the security measures of all third-party information management systems/digital platforms that we are using
- have risk management plan or data breach response plan in place that cover key strategies to mitigate cyber security incidents
- provide training to all workers that covers:
    - data collection and handling
    - data access and editing
    - data deletion and disposal
    - common data security, risks and scams (e.g. phishing emails, fake websites, technical support scams.)
    - key data protection practices (e.g. log in credentials, multi-factor authentication, system updates, anti-virus software, data-backups)
    - steps to take during a data breach incident
    - data breach reporting obligations
- ensure participants feel supported to access their data and provide feedback around our data handling
- only provide participant data to workers and other external parties (e.g. health service providers) that need access to this information
- comply with the following relevant policies:
    - Privacy and Confidentiality
    - Information security
    - Maintenance, records and audit
- comply with all relevant regulations and legislation including:
    - The Privacy Act 1988 (Cth)
    - Australian Privacy Principles (APP)
    - Legislation and regulations relevant to our state

incorporate data safety into the governance of our organisation.

Under the **Notifiable Data Breach (NDB) Scheme**, all notifiable data breaches must be reported to the **Office of the Australian Information Commissioner (OAIC)**. A notifiable data breach is any breach of data that is likely to cause any person or organisation serious harm. Examples of serious harm include:

- identity theft
- risk of physical harm
- serious psychological harm
- harm of an individual's reputation
- loss of trust in our organisation
- financial loss
- legal and regulatory consequences.

In addition to the above, we must inform that NDIA at privacy@ndis.gov.au if participant information was compromised during a data breach. This includes participant ID, name and any other identifying information about a participant or their plan.

If a data breach significantly impacts our ability to comply with the requirements of our NDIS registration, we will notify the **NDIS Commission.**

We will take each data breach or suspected data breach seriously and respond immediately to contain, assess and remediate every incident on a case-by-case basis. When responding to a data breach or suspected data breach, we will:

- contain the breach to prevent any compromise of personal information
- assess the breach to gather facts and evaluate risks including potential harm to individuals and whether the breach requires reporting
- act where required to remediate any risk of harm
- notify individuals and (where required) the Office of the Australian Information Commissioner per the requirements of the NDB
- review the incident and consider continuous improvement actions to avoid future breaches.

4.0 Artificial Intelligence and Privacy

YBSS is committed to ensuring that the use of Artificial Intelligence (AI) tools across the organisation is consistent with our obligations under the Privacy Act 1988 (Cth), the Information Privacy Act 2009 (Qld), and the Australian Privacy Principles. This section is to be read in conjunction with Section 17.0 of the YBSS Information Communication and Technology Policy.

Transparency and collection

YBSS will be transparent about the use of AI tools when processing personal or sensitive information. Participants, employees, and volunteers will be informed through intake or onboarding processes when AI tools may be used in connection with their personal information. Only information that is necessary for a legitimate business purpose may be processed through an approved AI tool. The following are prohibited from entry into any AI tool:

- Participant personal and sensitive information, including health, disability, financial, and NDIS plan information
- Employee and volunteer personal information
- Any information classified as Confidential or Restricted under the YBSS data classification guidelines

Use, disclosure, and cross-border transfer

Personal information processed through AI tools must only be used for the purpose for which it was collected and in accordance with consents obtained. YBSS will not

use AI tools to disclose or transfer personal information to third parties without individual consent, except where required by law. All approved AI tools must store and process data within Australia. Prior to approval, third-party AI platforms must be assessed to confirm that personal information entered is not used for model training or other secondary purposes inconsistent with the original purpose of collection.

Data classification and AI tool use

Classification	Description	AI tool use
Public information	Information intended for public release with no privacy risk	May be used with approved AI tools
Internal information	Operational information not identifying individuals	Approved enterprise-tier tools only
Confidential information	Personal information, sensitive information, commercially sensitive data	Prohibited from use with any AI tool
Restricted information	Information subject to specific legal protection or where disclosure causes serious harm	Requires explicit CEO approval; generally prohibited

Security and human oversight

YBSS protects personal information processed through AI tools by ensuring that:

- Only approved enterprise-tier tools with appropriate data controls are used where business information is involved
- All authorised users complete required training in data security, privacy, and ethical AI use before accessing approved tools
- All AI-generated outputs involving personal information are reviewed by a human before any action is taken or content distributed
- AI tools must not be used to make decisions about a participant's eligibility, service delivery, or support needs without human oversight and professional judgement
- Any AI-generated content recorded in a participant's file must be identified as such, verified for accuracy, and reviewed by an authorised worker

Participant privacy

Given the sensitivity of NDIS participant information and YBSS's obligations under the NDIS Practice Standards, participant personal and sensitive information must not be entered into any AI tool, including approved productivity tools. AI tools must not be used to replace or substitute informed consent processes, risk assessments, or safety planning in relation to participants.

AI-related privacy incidents

- A privacy breach involving an AI tool is an incident for the purposes of this policy and the YBSS ITC Policy. The following must be reported immediately to the relevant manager and the IT Department:
- Entry of personal, sensitive, confidential, or restricted information into an AI tool without appropriate authorisation
- AI outputs that disclose personal or sensitive information to unauthorised persons
- Use of a non-approved AI tool in connection with any YBSS information
- Any third-party platform breach that may have compromised information entered by YBSS users

All AI-related privacy incidents are managed in accordance with Section 3.0 of this policy. Where participant information is compromised, YBSS will notify the NDIA at privacy@ndis.gov.au. Where the breach meets the notifiable data breach threshold under the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), YBSS will notify the Office of the Australian Information Commissioner.

Responsibility and accountability

The CEO is responsible for ensuring AI tool use complies with this policy and applicable privacy legislation. The ICT Coordinator maintains the approved AI tools register and reviews the privacy practices of approved third-party platforms. All employees, volunteers, and contractors authorised to use AI tools are responsible for the appropriate handling of any information processed through those tools. A substantiated breach of privacy arising from AI tool use will result in disciplinary action consistent with the YBSS Code of Conduct.

5.0 How to contact us

Individuals can obtain further information in relation to this privacy policy, or provide any comments, by contacting us:

Yumba Bimbi: (07) 4987 7933
admin@yumbabimbi.com.au
PO Box 1607
Emerald QLD 4720