BRYMON PROMOTIONS

A Subsidiary of Brymon Consulting Pty Ltd

Supporting THE PLAY©, Voices That Matter© Youth Mental Health & Wellbeing Programme and Voices That Matter© App

PRIVACY, DATA PROTECTION & CONFIDENTIALITY POLICY

Australia and United Kingdom

Document owner	Director, Brymon Promotions
Version	1.0
Approval status	For formal adoption
Effective date	21 July 2026
Review date	21 July 2027 or earlier following legal or operational change
Classification	Public policy; controlled organisational document

This policy is an organisational governance document and not a substitute for jurisdiction-specific legal advice.

Document control and approval

Version	Date	Change	Approved by
1.0	21 July 2026	Initial Australia and United Kingdom policy	

Approval

Approved by	Brian Montgomery
Position	Director / Authorised Officer
Signature	
Date	21-07-2026

Controlled document notice

Printed or locally saved copies are uncontrolled unless marked and verified against the current approved version. Operational forms, privacy notices and consent wording must be reviewed whenever this policy changes.

Contents

1. Purpose and policy statement

Brymon Promotions is committed to respecting privacy, protecting personal information and maintaining confidentiality in every activity connected with THE PLAY©, Voices That Matter©, workshops, rehearsals, auditions, performances, events, fundraising, partnerships, online services and organisational administration.

The purpose of this policy is to establish a consistent, child-centred and risk-based framework for collecting, holding, using, disclosing, securing, retaining and disposing of personal information in Australia and the United Kingdom. It applies the higher practical standard where legal requirements differ, unless local law requires a different approach.

Core commitment
Brymon Promotions will collect only the information that is reasonably necessary, explain its purposes clearly, use it fairly, protect it appropriately, restrict access, respond to rights requests, and act promptly when information is lost, misused, or disclosed without authority.

Policy objectives

- protect the dignity, safety and autonomy of children, young people, families, workers and partners;
- meet applicable Australian and United Kingdom privacy and data-protection obligations;
- support safeguarding without allowing confidentiality to obstruct lawful information sharing;
- ensure transparent and age-appropriate privacy notices;
- reduce unnecessary collection, profiling and retention;
- establish practical controls for the Voices That Matter© App and other digital services;
- protect creative, commercial, contractual and organisational confidential information.

2. Scope

This policy applies to Brymon Consulting Pty Ltd, Brymon Promotions, THE PLAY©, Voices That Matter© and every director, employee, secondee, consultant, contractor, volunteer, facilitator, chaperone, student placement, artist, production worker and partner who handles information on Brymon's behalf.

It covers information relating to participants, prospective participants, parents, guardians, carers, staff, volunteers, applicants, cast members, audience members, donors, sponsors, schools, venues, suppliers, complainants, witnesses and users of websites, social media, mailing lists and apps.

The policy applies to paper, verbal, photographic, audio, video, electronic, cloud-hosted and device-based information, whether held directly by Brymon or by a service provider.

3. Legal and regulatory framework

3.1 Australia

The principal federal framework is the Privacy Act 1988 (Cth), including the Australian Privacy Principles and the Notifiable Data Breaches scheme. Coverage may depend on organisational status, turnover and activities. Brymon will nevertheless use the Australian Privacy Principles as its baseline governance standard, even where a statutory exemption may apply.

- Privacy Act 1988 (Cth) and Australian Privacy Principles;
- Notifiable Data Breaches scheme;
- Spam Act 2003 (Cth) and Do Not Call Register Act 2006 (Cth), where applicable;
- state and territory health-records, surveillance, child-protection, records and workplace laws where applicable;
- contractual privacy requirements imposed by schools, government agencies, venues, funders and partners;
- the emerging Children's Online Privacy Code framework, noting that final obligations must be reviewed when registered and commenced.

3.2 United Kingdom

The principal framework is the UK General Data Protection Regulation and the Data Protection Act 2018, supported by the Privacy and Electronic Communications Regulations where electronic marketing, cookies or similar technologies are used. Online services likely to be accessed by children must be designed consistently with the Information Commissioner's Children's Code.

- UK GDPR;
- Data Protection Act 2018;
- Privacy and Electronic Communications (EC Directive) Regulations 2003;
- ICO Children's Code / Age Appropriate Design Code;
- Human Rights Act 1998 and common-law confidentiality principles where relevant;
- applicable safeguarding, employment, charity, education and records obligations.

3.3 Policy interpretation

Where Brymon operates through a school, venue, council, charity or delivery partner, the parties must document whether each acts as an independent controller, joint controller, processor or service provider. Contract wording must not misstate legal responsibilities.

No blanket exemption
A small-business exemption, consent form or contractual disclaimer must never be treated as permission to handle information carelessly. Brymon's internal standard applies regardless of whether a regulator could exercise jurisdiction in a particular case.

4. Definitions

Term	Meaning
Personal information / personal data	Information or an opinion about an identified or reasonably identifiable individual. Under UK law, this includes information relating to an identified or identifiable natural person.
Sensitive information / special category data	Information requiring heightened protection, including health, disability, racial or ethnic origin, religious or philosophical beliefs, sexual orientation and certain biometric or genetic information.
Child / young person	For this policy, any person under 18, while recognising that legal capacity and online-consent rules vary by jurisdiction and circumstance.
Processing	Any operation performed on personal data, including collection, recording, use, disclosure, storage, alteration, analysis, transfer, archiving and destruction.
Controller	The person or organisation that determines the purposes and means of processing.
Processor/service provider	A party processing information on documented instructions for a controller or providing contracted services involving information.
Data breach	Loss, unauthorised access, disclosure, alteration, destruction or unavailability of information, whether accidental or deliberate.
Confidential information	Non-public personal, safeguarding, health, commercial, creative, financial, operational, security or partner information that must be protected from unauthorised use or disclosure.

5. Governance and accountability

The Director retains overall accountability for privacy governance. A Privacy Lead must be formally appointed before public launch of the Voices That Matter© App or any large-scale processing of children's data. A Data Protection Officer must be appointed where UK law requires one, including where core activities involve regular and systematic large-scale monitoring or large-scale processing of special-category data.

Roles

- Director / Authorised Officer: approves policy, resources compliance and receives serious incident reports.
- Privacy Lead: maintains records of processing, privacy notices, retention schedules, breach logs, rights requests and training.
- Safeguarding Lead: ensures privacy decisions support child safety and lawful information sharing.
- System owners: approve access, conduct reviews and ensure secure configuration.
- All personnel: follow need-to-know access, report incidents immediately and sign confidentiality obligations.
- Partners and processors: comply with contract, applicable law and Brymon instructions.

Records of processing

Brymon will maintain an information asset register and, where required, a record of processing activities that describes categories of individuals and data, purposes, lawful bases, recipients, transfers, retention periods, security controls, and responsible owners.

6. Privacy by design and data minimisation

Privacy must be considered before new programmes, forms, surveys, technologies, partnerships, marketing campaigns or app features are approved. Collection must be limited to what is proportionate and necessary for a defined purpose.

Privacy impact assessment triggers

- new app or digital service used by children;
- systematic monitoring, behavioural profiling or location data;
- large-scale health, safeguarding or special-category information;
- biometric identification, facial recognition or automated decision-making;
- new international transfers or high-risk cloud providers;
- matching or combining datasets;
- innovative technology with uncertain consequences;
- processing likely to create high risk to rights, safety or wellbeing.

A Data Protection Impact Assessment or Privacy Impact Assessment must identify necessity, proportionality, risks, mitigations, consultation needs, residual risk and approval. High residual UK risk must be escalated for ICO consultation where legally required.

7. Collection of personal information

Brymon may collect identification and contact details, age or date of birth, parent/guardian details, school information, attendance, emergency contacts, accessibility needs, health and medication information, safeguarding records, consent choices, audition material, performance participation, photographs, recordings, feedback, app activity, technical identifiers, payments and organisational correspondence.

Collection rules

1. Define the purpose before collection.
2. Use the least intrusive method.
3. Collect directly from the individual where reasonable.
4. Provide a concise privacy collection notice at or before collection.
5. Separate optional marketing and media choices from essential service information.
6. Avoid free-text fields where structured choices reduce unnecessary disclosure.
7. Do not request medical or safeguarding detail merely because it may be useful later.
8. Verify identity proportionately before changing or disclosing records.

Unsolicited information

Unsolicited information must be assessed promptly. If Brymon could not lawfully or reasonably have collected it and no legal retention duty applies, it must be securely destroyed or de-identified. Safeguarding disclosures must be preserved and escalated in accordance with safeguarding law and policy.

8. Children and young people

Children merit specific protection because they may be less able to recognise long-term privacy risks. Information must be presented in clear, age-appropriate language, and design choices must prioritise the child's best interests rather than engagement, advertising or data accumulation.

Minimum standards

- use layered notices: a short child-friendly summary plus full parent/adult information;
- assess the child's understanding and capacity rather than relying on age alone in Australia;
- apply UK rules on child consent for information-society services and seek parental authorisation where required;
- do not nudge children to weaken privacy settings or disclose more information;
- set high-privacy defaults;
- disable public profiles, precise geolocation and unnecessary contact by default;
- avoid behavioural advertising and commercial profiling of children;
- give children accessible routes to ask questions, correct information and seek deletion;
- involve safeguarding personnel where a rights request could expose a child to harm.

Safeguarding priority
Confidentiality is not absolute. Information may be shared without consent where necessary and lawful to protect a child or another person from harm, comply with reporting duties, prevent or investigate crime, or respond to an emergency. Only relevant information should be shared, with reasons recorded.

9. Lawful use and disclosure

Personal information may be used only for the notified purpose, a directly related or compatible purpose permitted by law, or another purpose supported by consent or lawful authority.

Common purposes

- registering and supporting participation;
- safeguarding, welfare and emergency response;
- delivering workshops, rehearsals, auditions and performances;
- reasonable adjustments and accessibility;
- communications with families, schools and partners;
- quality assurance, evaluation and funder reporting using aggregated or de-identified data where possible;
- contract, payment and accounting administration;
- security, fraud prevention and legal claims;
- approved marketing and media activities.

UK lawful bases

For UK processing, Brymon must document an Article 6 lawful basis and, where special-category data is processed, an Article 9 condition and any Data Protection Act 2018 requirement. Consent must not be selected where it is not genuinely optional or can be withdrawn without detriment. Legitimate interests require a recorded balancing assessment.

Disclosure register

Non-routine disclosures must record the date, recipient, information disclosed, authority, purpose, decision-maker and any restrictions. Bulk disclosures require Privacy Lead approval.

10. Sensitive, health and safeguarding information

Health, disability, mental-health, trauma, medication, cultural, religious, sexual-orientation and safeguarding information must receive enhanced protection. Access is restricted to personnel who need the information to perform an authorised role.

- store safeguarding case records separately from general participant files;
- use role-based permissions and audit logging where feasible;
- do not place detailed diagnoses on attendance lists, lanyards or general production schedules;
- communicate practical adjustments without disclosing underlying conditions unless necessary;
- share emergency medical details with first aiders or clinicians where required;
- do not promise secrecy when a disclosure raises safety concerns;
- record professional observations factually and distinguish them from allegations or opinions.

11. Consent and capacity

Valid consent must be informed, specific, freely given, current and capable of withdrawal. Silence, inactivity, bundled terms or pre-ticked boxes are not consent. Consent must be recorded with the notice version, date, method and scope.

Children

Australia does not prescribe a single age at which a child can make every privacy decision. Brymon will assess maturity and understanding and generally involve a parent or guardian for participants under 18, while respecting the young person's views and confidentiality where lawful and safe. In the UK, consent for online services offered directly to a child must meet the statutory age and parental-authorisation rules; other processing may rely on a different lawful basis.

Withdrawal

Withdrawal does not invalidate earlier lawful processing. Brymon must explain practical consequences, such as inability to publish a performance image or provide a feature that genuinely requires the information. Core participation must not be made conditional on optional marketing consent.

12. Photography, audio and video

Images and recordings may identify individuals and can expose children to misuse, unwanted contact or location disclosure. Brymon must use separate, granular media permissions and follow the Safeguarding & Child Protection Policy.

- obtain informed permission before planned identifiable filming or publication;
- explain channels, audience, duration and whether content may be promoted internationally;
- avoid publishing full names with images of children unless specifically justified and authorised;
- do not photograph changing areas, toilets, medical treatment or distress;
- use approved devices and transfer files promptly to authorised storage;
- honour refusals through practical arrangements such as non-filming zones;
- record withdrawal requests and remove future use where reasonably possible, while explaining limits for material already lawfully distributed or archived.

Audience photography

Event terms and signage may regulate audience photography, but signage alone does not replace appropriate permission for focused promotional use of identifiable children. Brymon may require audience members to stop recording and may remove persons who breach safety, privacy or venue rules.

13. Websites, apps, cookies and analytics

Websites and apps must publish clear privacy information and use proportionate tracking. Non-essential cookies or similar technologies must not be activated in the UK before valid consent where PECR requires it. Analytics settings should minimise identifiers, retention and cross-service sharing.

- maintain an accurate cookie and SDK inventory;
- block unapproved trackers;
- avoid advertising identifiers in children's services;
- use secure transmission and modern authentication;
- collect diagnostic logs only as necessary;
- provide account-deletion and privacy contact routes;
- review third-party SDK changes before deployment.

14. Voices That Matter© App controls

Before launch, the App must undergo privacy, safeguarding and security assessment. The App must not be treated as a clinical, emergency, or confidential counselling service unless it is separately designed, regulated, and resourced for that purpose.

Mandatory design controls

- high-privacy settings by default;
- age-appropriate onboarding and layered notices;
- parent/guardian involvement where required without automatically exposing a young person's private journal content;
- clear distinction between private journalling, information shared with Brymon and content visible to others;
- no open direct messaging between adults and children;
- moderation, reporting and escalation controls for community features;
- no precise location sharing;
- no sale of children's data;
- no behavioural advertising;
- minimum necessary analytics;
- encryption in transit and appropriate encryption at rest;
- documented account recovery and identity verification;
- defined crisis messaging explaining that emergency help must be sought through local services;
- retention limits for journal entries, messages, reports and inactive accounts;
- regular penetration testing and vulnerability management proportionate to risk.

Automated decisions and AI

Brymon will not make significant decisions about a child solely by automated means without a lawful basis, suitable safeguards, meaningful explanation and human review. Personal data must not be entered into public generative AI tools unless an approved contract, configuration, risk assessment, and lawful basis are in place.

15. Direct marketing and fundraising

Marketing must be fair, age-appropriate, and compliant with consent, opt-out, and electronic communications rules. Brymon Promotions must not exploit vulnerability or use sensitive or safeguarding information to target fundraising or promotional messages.

- maintain suppression lists;
- identify Brymon clearly;
- include a simple unsubscribe mechanism;
- obtain required consent before electronic marketing;
- keep sponsor communications separate from children's participation data;
- do not disclose mailing lists to sponsors for their independent marketing without a lawful basis and clear notice.

16. Confidentiality and professional conduct

All personnel owe duties of confidentiality. Access to information is granted for authorised work only and does not create a right to inspect, discuss, copy or retain information for personal purposes.

Prohibited conduct

- searching records out of curiosity;
- discussing cases in public or with unauthorised colleagues;
- using personal email, messaging or storage without approval;
- photographing screens or records;
- retaining participant lists after the task ends;
- sharing passwords or leaving devices unlocked;
- using confidential information for personal, commercial or creative advantage;
- publishing allegations, complaints or safeguarding information on social media.

Post-engagement obligations

Confidentiality continues after employment, volunteering, contracting or partnership ends. On departure, personnel must return or securely delete Brymon information, relinquish access and certify compliance when requested.

17. Schools, venues and partner organisations

Before sharing information with a school, venue, council, police service, charity or delivery partner, Brymon must define each party's role, purpose, lawful authority, permitted uses, security, retention, incident reporting and responsibility for rights requests.

- share the minimum necessary;
- use secure transfer methods;
- do not assume a school's consent covers Brymon's independent media or app use;
- record joint-controller arrangements where required;
- ensure emergency and safeguarding sharing is not delayed by contractual uncertainty;
- prohibit partner reuse for unrelated marketing or profiling.

18. Service providers and processors

Due diligence must be completed before a provider handles personal information. Contracts must address confidentiality, security, sub-processors, assistance with rights and breaches, deletion or return, audit rights and international transfers.

Minimum due diligence

- location of data and support access;
- security certifications and independent testing;
- breach history and response capability;
- child-data and advertising practices;
- retention and deletion functionality;
- sub-processor list;
- backup and disaster recovery;
- financial and operational resilience;
- ability to meet Australian and UK rights requirements.

19. Overseas transfers and cloud services

Cloud storage may result in overseas disclosure or restricted transfer. Brymon must identify storage and support locations and implement the mechanism required by applicable law.

Australia

Where APP 8 applies, Brymon must take reasonable steps before overseas disclosure and understand when it may remain accountable for the recipient's handling. Privacy notices must identify likely overseas locations where practicable.

United Kingdom

Restricted transfers must use an adequacy regulation, an appropriate safeguard such as an approved contractual mechanism, or a valid exception. Transfer risk assessments and supplementary measures must be documented where required.

20. Security controls

Security must be proportionate to sensitivity, scale, threat and potential harm. Controls include governance, people, physical, technical and supplier measures.

Baseline controls

- multi-factor authentication for privileged and remote access;
- unique accounts and least privilege;
- prompt access removal;
- device encryption and screen locks;
- approved password manager;
- secure backups and recovery testing;
- patching and vulnerability management;
- anti-malware and phishing protection;
- secure disposal of paper and devices;
- locked storage for paper records;
- encrypted transfer for sensitive files;
- logging and review of high-risk systems;
- annual access reviews and incident exercises.

Personal devices and remote work

Personal devices may be used only under approved conditions, with current security, lock screens, separate work storage and remote deletion where appropriate. Sensitive records must not be downloaded unnecessarily. Public Wi-Fi must not be used for sensitive work without an approved secure connection.

21. Access, correction and individual rights

Brymon will provide accessible channels for individuals to exercise rights. Requests must be logged, identity verified proportionately and answered within the applicable legal timeframe.

Australia

- access and correction under APPs 12 and 13 where applicable;
- complaint handling and explanation of review options;
- reasonable steps to notify prior recipients of corrections where required.

United Kingdom

- right to be informed;
- access;
- rectification;
- erasure;
- restriction;
- data portability where applicable;
- objection;
- rights relating to automated decision-making;
- complaint to the ICO.

Children's requests

A child may exercise rights in their own capacity where competent. A parent does not automatically have an unrestricted right to all information about a child. Brymon must consider authority, the child's best interests, confidentiality, safeguarding risk and applicable law before disclosure.

22. Retention and secure disposal

Information must not be kept indefinitely merely because storage is inexpensive. Retention must reflect purpose, legal obligations, safeguarding needs, limitation periods, contractual requirements and risk.

Indicative retention schedule

Record category	Indicative rule
Unsuccessful general enquiries	12 months after closure, unless consented to ongoing contact
Participant registration and attendance	7 years after last activity, subject to safeguarding and contractual needs
Child safeguarding and serious welfare records	Longer period determined by safeguarding law, limitation risk and professional advice; never destroy during an active concern or inquiry
Routine consent and media permissions	Duration of use plus 7 years
Financial and tax records	At least the statutory period applicable in the relevant jurisdiction
Recruitment records - unsuccessful	6 to 12 months unless law or consent supports longer
Worker personnel records	Employment/engagement plus applicable statutory and limitation period
App accounts and routine content	Defined by feature; inactive accounts reviewed for deletion, ordinarily within 24 months unless user-controlled retention or safety/legal hold applies
CCTV or security footage	Normally 30 days unless required for incident investigation
Complaints and incidents	7 years after closure, longer for child or serious matters

The approved retention schedule prevails over these indicative periods and must be legally reviewed before adoption. A legal, safeguarding, insurance or investigation hold suspends disposal.

Disposal

Paper must be cross-shredded or securely destroyed. Electronic records must be securely deleted from active systems and, where feasible, scheduled for expiry from backups. Devices must be sanitised before disposal or reuse.

23. Data breaches and incident response

All suspected loss, misdirection, unauthorised access, malware, account compromise, inappropriate disclosure, or system unavailability must be reported immediately to the Privacy Lead and, where children or safeguarding information is involved, to the Safeguarding Lead.

Immediate procedure

9. Protect people from immediate harm and contact emergency or safeguarding services where required.
10. Contain the breach without destroying evidence.
11. Preserve logs, messages, devices and relevant records.
12. Assess what happened, whose information is affected and likely consequences.
13. Notify insurers, affected partners and legal advisers as required.
14. Determine regulatory and individual notification duties.
15. Document decisions, even where notification is not required.
16. Remediate causes and monitor for further misuse.

Australia - Notifiable Data Breaches

Where the Privacy Act applies, Brymon must promptly assess suspected eligible data breaches. An eligible breach generally involves unauthorised access, disclosure or loss likely to result in serious harm that has not been prevented by remedial action. Required statements must be provided to the OAIC and affected individuals in accordance with law.

United Kingdom

A personal data breach must be notified to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it if it is likely to result in a risk to individuals' rights and freedoms. High-risk breaches must also be communicated to affected individuals without undue delay unless a lawful exception applies.

Strict reporting rule
No worker may delay reporting while trying to investigate privately, recover a device, contact the wrong recipient or avoid embarrassment. Internal escalation is immediate.

24. Complaints and regulatory cooperation

Privacy complaints will be acknowledged promptly, investigated impartially and answered in plain language. Brymon will not victimise a person for raising a concern or exercising a right.

Complaint pathway

17. Contact the Privacy Lead using the details in the current privacy notice.
18. Brymon acknowledges the complaint and identifies any immediate protection required.
19. Relevant records are secured and conflicts managed.
20. A written outcome explains findings, corrective action and review options.
21. Unresolved Australian complaints may be referred to the OAIC where jurisdiction applies. UK complaints may be referred to the ICO.

Regulators and lawful authorities will be assisted transparently. Nothing in a confidentiality agreement prevents protected reporting, legal advice, regulatory cooperation, safeguarding disclosure or whistleblowing protected by law.

25. Monitoring, training and review

Privacy induction is mandatory before access to personal information. Refresher training is required annually and following significant incidents or changes. Specialist roles receive additional training on children's data, safeguarding sharing, breach assessment, app operations and rights requests.

- annual policy review;
- quarterly review of high-risk incidents and overdue actions;
- periodic access and retention audits;
- supplier reviews;
- privacy testing of app releases;
- review of complaints and near misses;
- legal review when Australia's Children's Online Privacy Code is finalised or relevant UK law changes.

Appendix A - Privacy collection notice template

Who is collecting the information?

_____

What information is being collected?

_____

Why is it needed?

_____

Is collection required or optional?

_____

What happens if it is not provided?

_____

Who may receive it?

_____

Will it be stored or accessed overseas?

_____

How long will it be kept?

_____

What choices and rights are available?

_____

How can the person contact Brymon or complain?

_____

For children: short age-appropriate explanation and parent/guardian information.

_____

Appendix B - Confidentiality undertaking

I understand that I may receive personal, safeguarding, health, commercial, creative or operational information through my work with Brymon Promotions. I agree to access and use it only for authorised duties; protect it from loss or disclosure; follow policies and lawful instructions; report incidents immediately; return or delete it when directed; and maintain confidentiality after my role ends. This undertaking does not prevent lawful safeguarding reports, protected disclosures, regulatory cooperation, or the obtaining of legal advice.

Name: _____

Role/organisation: _____

Signature: _____

Date: _____

Appendix C - Data breach report form

Date and time discovered:

_____

Reported by and contact details:

_____

System, location or activity:

_____

What happened:

_____

Information involved:

_____

Number and categories of people affected:

_____

Children or vulnerable persons affected:

_____

Containment completed:

_____

Possible harm:

_____

Safeguarding or emergency action:

_____

Third parties notified:

_____

Regulatory assessment:

_____

Individual notification decision:

_____

Root cause:

_____

Corrective actions and owners:

_____

Closure approval and date:

_____

Appendix D - Data sharing checklist

☐ Purpose and necessity documented

☐ Lawful basis/authority identified

☐ Special-category condition identified where needed

☐ Best interests of child considered

☐ Minimum information selected

☐ Recipient identity and authority verified

☐ Secure method selected

☐ Contract or agreement checked

☐ Overseas transfer assessed

☐ Disclosure recorded

☐ Follow-up or deletion requirement agreed

Appendix E - Individual rights request log

Ref	Received	Requester	Right	ID check	Due	Outcome	Closed

Appendix F - Information asset register fields

- Asset/system name and owner
- Individuals and data categories
- Purpose and lawful basis
- Special-category condition
- Collection source and notice
- Recipients and processors
- Storage and access locations
- International transfers
- Retention and disposal
- Security classification and controls
- DPIA/PIA status
- Review date

Appendix G - References and authoritative guidance

Privacy Act 1988 (Cth), Federal Register of Legislation.

Office of the Australian Information Commissioner, Australian Privacy Principles and APP Guidelines.

OAIC, Data Breach Preparation and Response.

OAIC, Children and Young People - Privacy.

OAIC, Children's Online Privacy Code materials (draft/final status must be checked before reliance).

UK General Data Protection Regulation, as retained and amended.

Data Protection Act 2018 (UK).

Information Commissioner's Office, Children and the UK GDPR.

ICO, Age Appropriate Design: A Code of Practice for Online Services.

ICO, Personal Data Breaches: A Guide.

ICO, Data Sharing Code of Practice.

References checked against official sources in July 2026. This policy must be reviewed when legislation, regulatory guidance, organisational structure, service design or data flows change.

Appendix H - Contact and publication fields

Privacy Lead name: _____

Privacy email: _____

Postal address - Australia: _____

UK representative/contact if required: _____

Data Protection Officer if required: _____

Emergency breach escalation number: _____

Website privacy notice URL: _____

App privacy notice URL: _____

Before publication

Complete all contact fields; approve the retention schedule; confirm controller/processor roles; adopt an incident response team; review insurance and contracts; complete the App DPIA/PIA; and obtain jurisdiction-specific legal review.