Privacy Policy

Cutthru Pty Ltd, trading as Pollinate

Version: 1.1
Effective date: 23/03/2026
Review cycle: Biennial or upon material change
Policy owner: Howard Parry-Husbands
Contact: privacy@pollinate.com.au

1. Purpose

This Privacy Policy outlines how **Pollinate** manages information in the conduct of **market, opinion and social research**, in accordance with:

- **ISO 20252:2019** – Market, Opinion and Social Research service requirements
- **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**
- **The Research Society Code of Professional Behaviour**

The policy demonstrates our commitment to ethical research practice, confidentiality, appropriate information governance, and transparency with clients and research participants.

2. Scope

This policy applies to:

- All research activities conducted by **Pollinate**
- All Pollinate employees, directors, contractors and approved suppliers
- All research data, project materials, and client information handled by Pollinate

This policy does **not** apply to non-research activities such as direct marketing and sales outreach, or respondent recruitment, which are outside our business model.

3. Research model and data minimisation

Pollinate conducts research almost exclusively using **paid research-only panel suppliers**.

Key characteristics of our model:

- **No direct collection of respondent identities**
- **Limited receipt of names, phone numbers, or email addresses** e.g. for qualitative research (focus groups and interviews) participants opt-in to have their name and contact details shared with Pollinate for contact purposes
- Respondents sourced for online surveys are identified only via **unique, non-identifying codes** assigned by the panel supplier, and the data received is **de-identified** prior to transfer to Pollinate

- In some studies, **postcode or broad geographic indicators** may be included where analytically necessary
- Research participation is **voluntary,** and sensitive information is only collected where essential to the research project with explicit consent collected beforehand
- Research results are reported in **aggregated or de-identified** form

Panel suppliers are responsible for respondent recruitment, consent management, incentives, and identity handling.

This approach significantly reduces privacy risk and aligns with:

- **APP 1 (open and transparent management)**
- **APP 3 (collection of solicited information)**
- ISO 20252 principles of **confidentiality and proportionality**

4. Types of information we handle

4.1 De-identified research data

- Survey responses and qualitative materials
- Non-identifying demographic or profile attributes
- Supplier-assigned respondent reference codes
- Possible postcode (where required for research purposes)

4.2 Client and project information

- Client business contact details
- Research briefs and specifications
- Questionnaires, discussion guides, methodologies
- Analysis outputs, reports, and presentations

4.3 Operational and quality records

- Project documentation required for traceability
- Supplier agreements and statements of work
- System access logs and audit records (where applicable)

5. Collection methods

Information is obtained through:

- Secure transfer of de-identified datasets from approved panel suppliers
- Secure transfer of limited personal details for agreed contact purposes (e.g. to conduct an interview)

- Direct engagement with clients
- Generation of research materials and outputs during project execution

6. Use of information

Information is used strictly for:

- Conducting and managing the research project for which the information was supplied
- Analysis, interpretation, and reporting of research findings
- Quality assurance, auditability, and methodological transparency
- Meeting contractual, legal, professional, and ISO-related obligations

Information is **not** used for:

- Direct marketing
- Sales outreach
- Profiling outside the agreed research scope

7. Disclosure of information

Information may be disclosed to:

- **Clients**, in the form of aggregated or de-identified research outputs
- **Research panel suppliers**, as required for fieldwork execution
- **Technology and professional service providers** supporting secure operations
- **Regulators or authorities**, where legally required

We do not sell respondent data or disclose identifying information

8. Overseas data handling

Project data is stored within **Microsoft 365 SharePoint Online**, with the tenant being setup for data to reside in Australia only.

Where Microsoft subprocesses or services involve offshore data processing, we rely on:

- Microsoft's contractual privacy and security commitments
- Access controls, encryption, and tenant-level protections
- Risk-based assessment consistent with **APP 8 (cross-border disclosure)**

9. Information security

We maintain administrative, technical, and physical safeguards appropriate to the nature of the information we hold, including:

- Role-based access control and least-privilege access
- Multi-factor authentication for Microsoft 365
- Encryption in transit and at rest (where supported by the platform)
- Secure file sharing and transfer mechanisms
- Staff confidentiality obligations
- Internal incident reporting and response procedures

These measures support **APP 11 (security of personal information)** and ISO 20252 confidentiality requirements.

10. Data retention and disposal

Information is retained only for as long as necessary to fulfil research, contractual, and compliance requirements.

Standard retention periods (unless otherwise agreed):

- **General project records:**
  Minimum **12 months** after project completion
- **Research records required for traceability and replication:**
  Minimum **24 months** after project completion
- **Video, audio, or recorded qualitative research materials:**
  24 months, or as otherwise agreed in writing with the client

Client-specific retention periods override default periods where contractually agreed.

At the end of the retention period, information is securely deleted or de-identified in accordance with **APP 11 (security of personal information)**.

11. De-identification and re-identification controls

We prohibit attempts to re-identify individuals and apply safeguards to ensure re-identification risk remains **very low**, taking into account:

- Absence of direct identifiers
- Limited data granularity
- Aggregated reporting practices
- Controlled access environments

De-identification is treated as an ongoing risk-management process, not a one-off action.

12. Individual rights and enquiries

As **Pollinate** generally does not hold identifiable respondent information:

- Participant access, correction, or withdrawal requests should be directed to the **panel supplier**
- We will cooperate with suppliers where a request reasonably relates to data we hold

Privacy enquiries may be directed to:
privacy@pollinate.com.au

13. Complaints handling

If you believe your privacy has been interfered with:

1. Contact us in writing at **privacy@pollinate.com.au**
2. We will acknowledge your complaint and investigate promptly
3. If unresolved, you may escalate to the **Office of the Australian Information Commissioner (OAIC)**

14. Governance and ISO 20252 alignment

This policy supports our broader research governance framework by addressing:

- Confidentiality and independence of research
- Supplier and subcontractor controls
- Information handling and record management
- Defined roles, responsibilities, and review mechanisms

15. Policy review and updates

This policy is reviewed periodically and updated as required to reflect changes in:

- Legislation
- ISO standards
- Research practices
- Technology platforms

The current version is available upon request or via https://pollinate.com.au