DATA SECURITY POLICY
The Curiosity Company
Effective Date: 21 May 2025
Version: 1.0

---

1. Purpose

This policy outlines the principles and procedures for securing personal data handled by The Curiosity Company, a market and social insights consultancy. The Company is committed to complying with the **Privacy Act 2020 (New Zealand)** and the **Privacy Act 1988 (Commonwealth of Australia)**, including the **Australian Privacy Principles (APPs)** and **New Zealand Information Privacy Principles (IPPs)**.

---

2. Scope

This policy applies to all employees, contractors, researchers, interns, and third-party service providers who process or have access to personal data on behalf of the Company. It governs all personal data collected through:

- Research projects (e.g., surveys, interviews, panels, focus groups and in-depth interviews)
- Online tools, mobile platforms, or physical interactions
- Internal business operations and HR systems

---

3. Definitions

- Personal Information / Data: Any information about an identifiable individual, including names, email addresses, opinions, or any combination of information that can reasonably identify a person.
- Sensitive Information (Australia only): A special category of personal data (e.g. ethnicity, health data, political views) that requires higher protection.
- Data Subject / Individual: The person to whom the personal data relates.
- Data Controller (also known as “agency” in NZ): The organization that determines why and how personal data is processed.

---

4. Legal Framework and Principles

We are committed to collecting, storing, and handling personal data in line with the following:

- New Zealand Privacy Act 2020 (including the 13 IPPs)
- Australian Privacy Act 1988 (including the 13 APPs)
- Guidelines issued by the Office of the Privacy Commissioner (NZ) and the Office of the Australian Information Commissioner (OAIC)

---

5. Lawful Collection and Use:

- It is reasonably necessary for research purposes or business functions
- The individual has provided informed **consent**, where required
- The collection is directly related to the Company's legitimate business functions
- It is required or permitted by law

All collection is done transparently, with clear privacy notices and statements where appropriate.

---

6. Data Minimisation and Storage

We limit the collection of personal data to what is necessary for research or business purposes. Key practices include:

- Anonymising or de-identifying data where feasible
- Securely storing data in New Zealand, Australia, or trusted jurisdictions with adequate safeguards
- Ensuring personal data is retained **only as long as necessary**, after which it is securely deleted or de-identified in accordance with relevant laws

---

7. Security Safeguards:

We employ technical and organisational measures to protect personal data against loss, misuse, unauthorized access, modification, or disclosure.

Technical Measures

- Use of secure, encrypted data collection tools and servers
- Firewalls, endpoint protection, and two-factor authentication
- Role-based access and audit logging

Organisational Measures

- Regular staff training in data protection and ethical research practices
- Confidentiality clauses in employment and contractor agreements
- Procedures for secure data handling, including disposal and device management

---

8. Disclosure to Third Parties

We only disclose personal data to third parties where:

- The third party is contractually bound to comply with equivalent privacy standards
- Disclosure is necessary for research delivery, client reporting, or legal compliance
- The individual has consented, where appropriate

Where personal data is transferred outside New Zealand or Australia, we ensure the receiving jurisdiction has comparable privacy protections, or we use appropriate contractual safeguards.

---

9. Rights of Individuals

We uphold the rights of individuals under the NZ IPPs and AU APPs, including the right to:

- Access their personal information
- Request correction of inaccurate or incomplete information
- Withdraw consent (where applicable)
- Complain if they believe their privacy has been breached

Individuals may contact our Privacy Officer via:

Privacy Officer
The Curiosity Company
12 Gurners Lane
Lincoln
7608

Alternatively, you can email us at privacy@curiositycompany.co.nz or you can call us on **+64 22 140 8700**. We aim to respond within 14 working days from the date we receive privacy related communications.

---

10. Data Breach Response

In the event of a notifiable data breach, the Company will:

- Contain the breach and assess the impact
- Notify affected individuals if there is a risk of serious harm (AU) or serious privacy risk (NZ)
- Report the breach to the OAIC (Australia) or the Privacy Commissioner (New Zealand), if required
- Maintain an internal breach register

---

11. Monitoring and Review

This policy is reviewed annually or when legislative or operational changes occur. Revisions are approved by senior management and communicated to all employees and partners.

Approved by: Ann Thompson