

THE LEADERSHIP CONTEXT PTY LTD

Data Protection & Technology Risk Policy

ABN: [52 636 526 808]

Policy Owner	Principal / Managing Director
Version	1.0
Effective Date	December 2025
Review Date	December 2027
Jurisdiction	Commonwealth of Australia
Applicable Law	Privacy Act 1988 (Cth); Australian Privacy Principles (APPs)

1. Purpose

This Policy sets out how The Leadership Context Pty Ltd ("the Company", "we", "us") collects, uses, stores, protects, and disposes of personal information, and how we manage technology-related risks in our executive coaching practice. It reflects our obligations under the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

This Policy applies to all staff, contractors, coaches, and any third parties who access Company systems or handle personal information on our behalf.

2. Scope

This Policy applies to all personal information we hold, including:

- Client and prospective client information (names, contact details, employment information, coaching session notes, psychometric or assessment data)
- Business contact information
- Employee and contractor information
- Information held in digital systems, cloud platforms, email, mobile devices, and physical records

3. Information We Collect and Why

3.1 Types of Personal Information

We collect personal information that is reasonably necessary to provide executive coaching services, including:

- Identity and contact details (name, email address, phone number, employer, role)
- Coaching and professional development information (goals, challenges, 360-degree feedback, assessment results)

- Sensitive information where relevant and consented to (e.g. health information that bears on coaching objectives)
- Payment and invoicing information

3.2 How We Collect Information

We collect information directly from clients and organisations at the point of engagement, through intake forms, coaching sessions, and assessments. We do not collect personal information by unlawful means.

3.3 Purpose of Collection

Personal information is collected solely for the purposes of:

- Delivering executive coaching and consulting services
- Administering client relationships, invoicing, and scheduling
- Improving our services and conducting research (in de-identified form where applicable)
- Complying with legal and contractual obligations

We will not use personal information for a secondary purpose without consent, unless permitted by law.

4. Data Protection & Security

4.1 Storage and Access Controls

The Company takes reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. Our security measures include:

- Password-protected and encrypted devices for all business use
- Secure cloud storage with access limited to authorised personnel (e.g. Google Workspace or Microsoft 365 with multi-factor authentication enabled)
- Secure video conferencing platforms for coaching sessions (e.g. Zoom, Teams) with waiting rooms and session controls enabled
- Session notes and sensitive client files stored in encrypted folders, not local desktops
- Physical documents containing personal information stored in locked storage and securely disposed of when no longer required

4.2 Data Retention

We retain personal information only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. As a general guide:

- Active client files: retained for the duration of the engagement plus seven (7) years
- Financial records: retained for seven (7) years in accordance with taxation law
- Unsuccessful business enquiries: deleted or de-identified within twelve (12) months

When personal information is no longer required, it will be destroyed or de-identified in a secure manner.

4.3 Third-Party Service Providers

We may share personal information with trusted third-party providers (e.g. assessment platforms, scheduling tools, accounting software) only where necessary and subject to

appropriate data processing agreements. We take reasonable steps to ensure third parties handle personal information in accordance with the APPs.

We do not sell or trade personal information to any third party.

5. Technology Risk Management

5.1 Acceptable Use of Technology

All staff and contractors must:

- Use strong, unique passwords for all business systems and enable multi-factor authentication wherever available
- Keep all devices, operating systems, and applications updated with current security patches
- Use only Company-approved platforms and applications when handling client data
- Avoid accessing client data on public or unsecured Wi-Fi networks without a VPN
- Not store client information on personal devices unless explicitly authorised

5.2 Artificial Intelligence (AI) Tools

Given the increasing use of AI tools in business operations, the following rules apply:

- Personal or sensitive client information must not be entered into public AI platforms (e.g. ChatGPT, Gemini, or similar) without client consent and confirmation that data will not be used for model training
- Any AI tools used in the delivery of coaching services must be disclosed to clients
- AI-generated content used in coaching engagements must be reviewed and verified by the coach before use
- Staff should remain alert to AI-related risks including data leakage, inaccurate outputs, and over-reliance on automated tools

5.3 Device Loss or Theft

In the event of a lost or stolen device containing client data, the incident must be reported immediately to the Policy Owner. Remote wipe capabilities should be enabled on all mobile devices used for business purposes.

5.4 Breach Response

In the event of a suspected or actual data breach, the Company will:

1. Contain the breach as quickly as possible
2. Assess the likely harm to affected individuals
3. Notify the Office of the Australian Information Commissioner (OAIC) if the breach is likely to result in serious harm (as required under the Notifiable Data Breaches scheme)
4. Notify affected individuals where required or appropriate
5. Review and remediate the circumstances that led to the breach

A record of all data breaches and responses will be maintained by the Policy Owner.

6. Access, Correction, and Complaints

6.1 Access and Correction

Individuals have the right to request access to personal information we hold about them, and to request corrections where the information is inaccurate, out of date, incomplete, or misleading. Requests can be made by contacting us at the details below. We will respond within a reasonable timeframe (generally 30 days).

In limited circumstances, we may decline access where permitted under the Privacy Act 1988 (Cth), and we will provide written reasons for any refusal.

6.2 Complaints

If you believe we have mishandled your personal information, please contact us in the first instance. We will investigate and respond within 30 days. If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

7. Roles and Responsibilities

Role	Responsibility
Policy Owner / Principal	Maintain and review this Policy; manage breaches; respond to access requests and complaints
All Staff & Contractors	Comply with this Policy; report breaches or concerns promptly; complete training as required
Third-Party Providers	Handle personal information in accordance with their contractual obligations and applicable law

8. Policy Review

This Policy will be reviewed annually, or sooner in the event of a significant change to our operations, a data breach, or a change in applicable law. The current version will be available to clients and staff on request.

9. Contact Us

For privacy-related enquiries, access requests, or complaints:

The Leadership Context Pty Ltd

Attn: Privacy Officer / Principal

Email: padraig@theleadershipcontext.com

Website: www.theleadershipcontext.com

Legal Disclaimer

This Policy has been prepared for The Leadership Context Pty Ltd as a practical compliance document. It is intended as a reasonable and proportionate response to obligations under the Privacy Act 1988 (Cth) for a small business in the executive coaching sector. It does not constitute legal advice. The Company should seek

independent legal advice if it handles sensitive information at scale, operates internationally, or is subject to additional regulatory obligations.