Premedia Responsible Information Management Policy

Premedia Marketing Production Services Pty Ltd
ABN: 61 647 912 150
Address: PO Box 341 Hornsby NSW 1630 Australia
Phone: 1800 571 825

Effective Date: 1st July 2025
Reviewed: Annually
Approved by: Mike Griffiths, Managing Director

---

1. Policy Statement

Premedia is committed to the responsible management of information, encompassing personal, commercial, and operational data across all business functions. We recognise the importance of maintaining confidentiality, ensuring data integrity, and protecting against unauthorised access, disclosure, or misuse.
We are guided by the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) and take reference from the General Data Protection Regulation (GDPR) for best practice in handling personal data.

---

2. Qualitative Objectives

- Maintain zero tolerance for data misuse, corruption, or unauthorised disclosure.
- Ensure compliance with applicable privacy laws and client confidentiality agreements.
- Promote transparency in how we collect, use, and manage information.
- Guarantee that staff understand and follow data protection and privacy responsibilities.

3. Quantitative Targets

Metric	Target	Frequency
Data breach or unauthorised disclosure	0 incidents per year	Ongoing
Employee privacy & data security induction	100% completion within 30 days	Onboarding & annually
Review of data handling processes	1 per financial year	Annual review
Records stored securely	100% of records retained 7+ years	Annual audit
Backup and recovery checks	100% systems verified quarterly	Quarterly

---

4. Scope and Application

This policy applies to all Premedia personnel, including the Director, contractors, and virtual assistants. It governs all internal and external information, including but not limited to:

- Client artwork, briefs, brand assets, and quotes
- Personal data (names, email addresses, payment information, etc.)
- Business records, tax documentation, and employment-related files
- Supplier, contractor, and partner information
- Website form submissions, CRM entries, and eCommerce data

---

5. Information Collection and Handling

We collect personal and business information via email, online forms, client conversations, and order systems. This data is used solely for operational purposes (project delivery, invoicing, customer service, and compliance).

Information uses include:

- Order processing
- Project communication
- Regulatory reporting
- Marketing (opt-in only)

We do not sell or share personal data with third parties.

6. Data Protection Controls

Access Control:

- Access to data is restricted to authorised personnel (Mike, Kate, and designated VA)
- Strong passwords, 2FA, and secure device usage are enforced

Data Storage:

- Cloud-based systems (e.g. Google Workspace, Xero, HubSpot) are used
- Local devices are encrypted and regularly updated

Data Retention:

- Business records are kept for a minimum of 7 years
- Marketing data is reviewed and cleaned every 12 months

Disposal of Data:

- Digital files are permanently deleted when no longer needed
- Paper documents are shredded using cross-cut shredders

---

7. Breach Management

If a data breach or suspected breach occurs:

1. Immediate investigation is triggered (within 24 hours)
2. Affected parties are notified (as required by the Notifiable Data Breaches (NDB) Scheme)
3. Incident details are logged and stored securely
4. Control measures are reviewed and improved as necessary

---

8. Employee and Contractor Responsibilities

All staff and contractors are expected to:

- Complete privacy and data awareness induction
- Report suspected data security issues immediately
- Maintain confidentiality of client and business information
- Use approved tools and follow secure handling protocols

9. Third Party Tools and Partners

We ensure any third-party platforms used (e.g. HubSpot, Canva, Google Workspace, Xero) align with privacy compliance obligations. Where appropriate, Data Processing Agreements (DPAs) are reviewed and accepted.

---

10. Review and Improvement

This policy will be reviewed annually or earlier if:

- Business operations change
- New legal obligations emerge
- A data incident requires policy revision

We welcome client and partner feedback to improve our approach to data protection.