POLICY DOCUMENT

PRIVACY POLICY

VERSION: 1.1

Table of Contents

1. INTRODUCTION

1.1 Purpose

The purpose of this policy is to outline how Sydney Markets Limited (SML) collects, uses, discloses, manages, secures, and disposes of personal and sensitive information. SML is fully committed to protecting the privacy of the information collected and strictly complies with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs. This policy details SML's obligations regarding the entire information lifecycle, from collection to secure destruction or de-identification.

1.2 Scope

This policy applies to all personal and sensitive information obtained from tenants, contractors, suppliers, visitors, employees, prospective employees, and other stakeholders involved with or engaged by SML for tenancy management, operations, safety compliance, event management, and other essential business functions. This includes all operational areas, common areas, and leased spaces within Sydney Markets premises, as well as data collected through our website and digital platforms.

This policy does not apply to activities or areas explicitly governed by separate, overriding agreements or legislative frameworks beyond SML's direct control.

1.3 Policy References

This policy was developed with references to the following documents or legislation:

Document Name	Link
Privacy Act 1988 (Cth)	www.legislation.gov.au
Australian Privacy Principles (APPs)	www.oaic.gov.au
Work Health and Safety Act 2011 (NSW)	www.legislation.nsw.gov.au
The Surveillance Devices Act 2007 (NSW)	https://legislation.nsw.gov.au/

1.4 Contact Information

Privacy Officer Sydney Markets Ltd

Email: privacy@sydneymarkets.com

Phone: 9325 6215

Mail: Level 3, Market Plaza Building, Parramatta Rd, SYDNEY MARKETS NSW 2129

1.5 Definitions

Term	Definition
Biometric Data	Unique biological or behavioural characteristics used for identification, such as facial recognition templates. It refers to data collected via facial recognition technology, which is Sensitive Information and afford higher protection under the Privacy Act.
Facial Identification	refers to 'one-to-one' matching. It involves determining whether a face matches a single biometric template. An example is iPhone Face ID.
Facial recognition	refers to 'one-to-many' matching. It involves determining whether a face matches any biometric template in a database. Facial identification is increasingly used by law enforcement to identify an unknown criminal suspect by comparing their faces that appear in databases.
Licensees	refers to all Occupiers, Licensees and visitors to the premises who are bound by the Market Rules and Regulations
Notifiable Data Breach	An eligible data breach that is likely to result in serious harm to any of the individuals to whom the information relates, and SML has not been able to prevent the likely risk of serious harm with remedial action.
Personal Information	Identifiable information about an individual, including names, birth dates, contact details, identification documents, employment records, financial details, vehicle or licence particulars, and biometric data (e.g., facial recognition templates).
Sensitive Information	Includes, but is not limited to, health and medical data, COVID-19 vaccination records, drug and alcohol testing outcomes, criminal background checks, and other information gathered with explicit consent or as mandated by law. This also encompasses biometric information used for identification and access control where it reveals sensitive details.
De-identification	The process of removing or modifying personal information so that an individual cannot be reasonably identified from the information.
SML Premises	Refers to all land, buildings, and facilities owned, operated, or managed by Sydney Markets Limited.

2. POLICY STATEMENT

Sydney Markets Limited is dedicated to protecting the privacy of all individuals interacting with its operations and premises. We are committed to maintaining transparent practices regarding the collection, use, and disclosure of personal and sensitive information, ensuring strict compliance with Australian privacy laws. Our policy prioritises safety, security, and operational efficiency while upholding individual privacy rights throughout the entire data lifecycle.

3. POLICY REQUIREMENTS

The key elements of this policy are as follows:

3.1 Collection of Personal and Sensitive Information

SML collects personal and sensitive information through fair and lawful means, ensuring that individuals are aware of the purpose of collection and their rights.

3.1.1 Methods of Collection

SML acquires information through:

- Direct Interaction – completed forms, signed agreements, inductions, inquiries, emails, telephone communications and direct interactions with SML employees.
- Telephone communications – recorded inbound and outbound telephone communications to support operational integrity, quality assurance, staff training, incident investigation and compliance with legal obligations.
- Security Measures
    - CCTV Monitoring - Continuous camera surveillance operates across SML premises for safety, security, and incident investigation purposes. This surveillance captures images and video of staff, Tenants, Licensees, contractors, and the public. Signage is prominently displayed around the premises to notify visitors that CCTV monitoring is in operation. By entering the site, you acknowledge and consent to surveillance for the purposes stated.
    - Site Access Control Systems - These systems record entry and exit times and may involve the use of identification cards, Facial Identification, Vehicle Licence Plate Recognition or Biometric Data (Facial Recognition).
    - Biometric Data Collection (Facial Recognition): For enhanced security and streamlined access, SML may collect biometric data (specifically facial recognition templates) from consenting Tenants, Licensees, their staff, and SML employees. This data is collected with explicit, informed consent and used solely for identity verification and access control on SML premises. Individuals providing biometric consent will be fully informed of the purpose, storage, and security of this data.
- Drug and Alcohol Testing – Regular, random, targeted, incident-triggered, or compliance-required drug and alcohol tests are performed on-site. By accessing SML sites, individuals explicitly consent to participate in drug and alcohol testing as required for safety, compliance, or incident investigation.

- Third-Party Sources - Including employers (e.g., for contractors and their staff), credit reporting bodies, governmental databases, and referrals from trusted sources, where permitted by law or with consent.
- Website Interactions
    - Cookies - SML's website uses cookies to optimise website functionality and user experience. Users are notified about the use of cookies upon visiting the website, typically through a banner or pop-up, and are given options to manage their cookie preferences where applicable.
    - Analytics Tools - Tools collect anonymous data about website usage (e.g., IP addresses, browse patterns, referral sites) to improve online services and understand user behaviour. No attempt will be made to identify anonymous users or their Browse activities unless legally compelled to do so.
- Online Forms - Information submitted via online forms (e.g., contact forms, event registrations, service requests) is collected directly from the individual. A privacy collection notice will be provided at the point of collection, outlining the specific purpose of data collection.

3.1.1.a Telephone Communications – Call Recording and Consent

SML may record inbound and outbound telephone communications to support operational integrity, quality assurance, staff training, incident investigation, and compliance with legal obligations. These recordings are governed by the *Surveillance Devices Act* 2007 (NSW) and the *Privacy Act 1988* (Cth), including the Australian Privacy Principles (APPs).

Consent is obtained through either express or implied means. Express consent is provided verbally or in writing. Implied consent is inferred when individuals are notified that the call may be recorded and continue with the conversation without objection.

For inbound calls, callers are notified via an automated message at the beginning of the call. For outbound calls, SML representatives inform the recipient at the start of the conversation. Individuals who object to recording may request alternative communication methods, such as written correspondence or unrecorded calls.

Call recordings are used strictly for quality assurance, training, compliance, incident investigation, and protection of SML's lawful interests. Recordings are stored securely, accessed only by authorised personnel, and retained in accordance with SML's data retention policies.

3.1.2 Notification of Collection

At or before the time of collecting personal information (or as soon as practicable thereafter), SML will take reasonable steps to ensure individuals are aware of:

- SML's identity and contact details.
- The fact and circumstances of the collection.
- Whether the collection is required or authorised by law.
- The purposes for which the information is collected.

- The main consequences if the information is not collected.
- The types of organisations or persons to which SML usually discloses personal information of that kind.
- Information about SML's Privacy Policy (this document).
- How to access and correct personal information, and how to make a complaint.

3.1.3 Anonymity and Pseudonymity

Where practicable and lawful, individuals will have the option of not identifying themselves, or of using a pseudonym, when dealing with SML. However, for most operational and safety-related activities on SML premises (e.g., site access, tenancy, employment), identification is a necessary requirement.

3.2 Usage of Personal and Sensitive Information

SML uses personal and sensitive information only for the purposes for which it was collected, or for directly related secondary purposes that the individual would reasonably expect or where required or permitted by law.

3.2.1 Primary Purposes of Use

Collected information enables SML to:

- Fulfill comprehensive workplace health and safety obligations, including drug and alcohol testing protocols.
- Administer tenancy, licensing and registration agreements and their underlying processes efficiently.
- Ensure site security and uphold regulatory compliance, and manage site entry and access control, including the use of CCTV and biometric data.
- Investigate and address incidents thoroughly.
- Communicate operational updates and essential notices effectively.
- Manage financial transactions, credit checks, and legal compliance seamlessly.
- Process employment applications, onboarding, and manage contractors effectively.
- Process tenant, licensee and Tenant or licensee induction and identification (for the principal and their employees and contractors) to facilitate access, track movements, and ensure compliance with Market Rules and Regulations and safety standards.
- Detect and prevent fraudulent, unlawful, or unsafe activities proactively.
- Enhance website functionality and user experience (for website data).
- Record and review telephone communications for quality assurance, training, compliance, incident investigation and lawful interest protection.

3.2.2 Secondary Purposes of Use

SML may use information for secondary purposes that are related to the primary purpose of collection and are within the reasonable expectations of the individual (or directly related in the case of sensitive information), or where consent is obtained, or as permitted by law. Examples include:

- Internal auditing and reporting.
- Improving SML's services and operations.
- Statistical analysis (often using de-identified data).

3.3 Information Disclosure

SML may disclose Personal and Sensitive Information to:

- Approved Contractors and Service Providers - Including security, IT, mailing, and marketing agencies, who assist SML in its operations and are bound by confidentiality agreements.
- Professional Advisors - Such as legal counsel, safety advisors, and accountants, for professional advice and compliance.
- Government and Regulatory Bodies - As legally required or authorised (e.g., to the police, work health and safety authorities, or in response to a court order). This includes disclosure of drug and alcohol testing outcomes to relevant regulatory authorities if mandated.
- Employers, Insurers, and Legal Representatives - For incident management, compliance enforcement, and workplace safety assurance, particularly concerning drug and alcohol testing outcomes or incidents captured by surveillance.
- Third-party providers for biometric data processing - Where biometric data is collected, it may be shared with secure third-party service providers solely for the purpose of identity verification and access control. These providers are required to adhere to strict data security and privacy standards and handle data in accordance with Australian privacy laws.
- Other Market Stakeholders - Where necessary for the legitimate operation of the markets and with appropriate privacy safeguards (e.g., sharing contact details of a tenant or licensee with another tenant or licensee for a legitimate business purpose with consent).
- Internal teams and authorised external parties for the review and use of recorded telephone communications, strictly for operational, legal and compliance purposes.

3.3.1 Cross Border Disclosure

SML generally does not disclose personal information to overseas recipients. If such a disclosure becomes necessary, SML will take reasonable steps to ensure that the overseas recipient handles the personal information in accordance with the Australian Privacy Principles, unless SML obtains the individual's informed consent after expressly advising them that APP 8.1 will not apply.

3.4 Data Security Measures

SML employs stringent security measures, both technical and organisational, to protect personal information from unauthorised access, disclosure, loss, or misuse. These measures include:

- Encryption – Use of encryption for electronic storage and transmission of sensitive information.
- Access Controls – Strict access controls and authentication mechanisms to limit access to personal information to authorised personnel only, based on their roles and responsibilities.
- Physical Security – Controlled physical access to data storage facilities and SML premises where personal information is held.
- Network Security - Firewalls, intrusion detection systems, and regular vulnerability assessments to protect SML's IT systems.
- Regular Audits – Periodic security audits and reviews to identify and address potential vulnerabilities and ensure ongoing compliance.
- Staff Training – Mandatory and regular privacy and data security training for all SML staff handling personal and sensitive information.
- Tenants and Licensees Management – Ensuring that third-party service providers who handle SML's personal information adhere to equivalent or higher privacy and security standards through contractual agreements.

3.5 Retention and Retirement of Information

SML retains personal information only for as long as necessary to fulfil the purposes for which it was collected, or as required by law.

Retention Periods

- Statutory Requirements - Information will be retained for periods mandated by relevant Australian laws and regulations (e.g., tax records, workplace health and safety records, employment records).
- Operational Necessity- Information will be retained for as long as it is reasonably necessary for SML's business functions and activities, including managing ongoing relationships with tenants, Licensees, contractors, and employees.
- Incident and Litigation Management - Information relevant to potential or ongoing investigations, disputes, or legal proceedings may be retained for longer periods as required.

3.5.1 Retirement (Destruction or De-identification)

Once personal information is no longer needed for any purpose for which it may be used or disclosed under the APPs (and no legal requirement for retention applies), SML will take reasonable steps to:

- Destroy the information in a secure manner (e.g., shredding paper documents, securely wiping electronic data) to prevent unauthorised access or reconstruction.
- If the information is to be retained for statistical analysis or research, SML will take reasonable steps to de-identify it so that the individual cannot be reasonably identified from the information. This involves removing direct identifiers and altering or removing other information that could lead to re-identification.

3.6 Access and Correction Rights

Individuals have the right to request access to, or rectification of, their personal information held by SML by contacting the Privacy Officer. Requests will be processed promptly (within 30 days) unless specific exceptions apply under applicable legislation. SML will take reasonable steps to ensure the information it holds is accurate, complete, relevant, up-to-date, and not misleading, having regard to the purpose for which it is held. If SML refuses a request for access or correction, it will provide written reasons for the refusal and information about how to make a complaint.

3.7 Privacy Complaints Process

All privacy-related complaints should initially be directed to the Privacy Officer. SML is committed to resolving complaints fairly and efficiently. SML will acknowledge receipt of a complaint promptly and endeavour to provide a substantive response within 30 days. If a satisfactory resolution is not achieved, complaints may be escalated to the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

3.8 Notifiable Data Breaches

In the event of an eligible data breach that is likely to result in serious harm to any individual whose personal information SML holds, SML will comply with its obligations under the Notifiable Data Breaches (NDB) scheme by:

- Carrying out a swift assessment of the suspected breach.
- Notifying affected individuals and the OAIC as soon as practicable if an eligible data breach is confirmed.
- Taking all reasonable steps to mitigate harm to affected individuals.

3.9 Marketing and Communications

SML may use collected information to deliver operational notifications and targeted marketing communications. You retain the right to opt-out from receiving marketing communications at any time by contacting our Privacy Officer or by using the opt-out mechanism provided in the communication. SML will not use or disclose sensitive information for direct marketing without explicit consent.

3.10 Policy Updates

SML may revise this policy periodically to ensure continuous compliance with changing laws, technologies, and practices. The latest version will always be accessible at www.sydneymarkets.com/home/privacy.

4. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Board of Directors	Oversees SML's overall compliance with privacy obligations and approves major policy revisions.
CEO/Management	Ensures adequate resources are allocated for privacy compliance, fosters a culture of privacy protection, and approves significant changes to privacy practices.
Privacy Officer	Serves as the primary contact for privacy enquiries and complaints. Manages privacy compliance programs, oversees data breach response, provides advice on privacy matters, and ensures staff training. Responsible for reviewing and approving data retention and retirement schedules.
Head of Technology	Implements and maintains technical security measures, manages data storage and access controls, assists with data breach investigations, and ensures secure destruction/de-identification of electronic data.
Head of People & Culture	Manages employee privacy issues, including employment records and drug and alcohol testing data for staff, and ensures compliance with privacy in recruitment and onboarding.
Head of Operations	Manages CCTV surveillance, site access control systems, drug and alcohol testing procedures, and ensures staff operating these systems are adequately trained and comply with privacy protocols. Responsible for physical security of data and secure destruction of physical records.
All Employees, Contractors, Tenants, Licensees and Visitors	Understand and adhere to this policy, report any suspected privacy breaches or concerns to the Privacy Officer, and provide accurate and complete information when requested by SML. Explicitly consent to drug and alcohol testing on request and, where applicable, biometric data collection as a condition of accessing or operating on SML premises.

5. NON-COMPLIANCE AND CONSEQUENCE

5.1 Failure to Comply

Failure to comply with this policy may result in disciplinary action for employees, including but not limited to verbal warnings, written warnings, or termination of employment.

For contractors and market participants, non-compliance may lead to penalties or termination of their occupancy agreements with Sydney Markets Ltd. Serious breaches may also result in legal action. Breaches of privacy laws, including the *Privacy Act 1988* (Cth), may also lead to significant penalties imposed by regulatory bodies (e.g., fines by the OAIC).

5.2 Escalation

All instances of non-compliance will be investigated. Suspected breaches of this policy or privacy laws will be immediately reported to the Privacy Officer. Depending on the nature and severity of the non-compliance, escalation may involve internal management, legal counsel, and, where a Notifiable Data Breach has occurred, the OAIC.

6. POLICY IMPLEMENTATION

6.1 Policy Distribution & Training

This policy will be made available to all SML employees, contractors, tenants, Licensees and relevant stakeholders through the SML website and during induction processes. Regular training sessions will be conducted for staff to ensure they understand their obligations under this policy and relevant privacy laws. Specific training will be provided for staff involved in handling sensitive information, conducting surveillance, managing biometric data, or handling website user data.

7. REVIEW AND AMENDMENT

This policy will be reviewed by the Policy Owner annually or sooner if there are changes in legislation, operational practices, or significant incidents (e.g., major data breaches).

Any amendments to this policy must be approved by the SML Board of Directors.

8. REPORTING REQUIREMENTS

All privacy-related incidents, including suspected data breaches, must be reported immediately to the Privacy Officer. The Privacy Officer is responsible for assessing incidents, initiating investigations, and reporting eligible data breaches to the OAIC in accordance with the Notifiable Data Breaches scheme. Regular reports on privacy compliance and incidents will be provided to the CEO and Board of Directors by the Privacy Officer.

9. CONFIDENTIALITY

All personal and sensitive information collected by SML will be treated with strict confidentiality. SML employees, contractors, and agents are bound by confidentiality obligations and are prohibited from accessing, using, or disclosing personal information except as authorised by this policy or by law.