

## Privacy Policy

HRM-POL-L-034

Uncontrolled if printed

3	12.05.25	'NATIONAL PRIVACY PRINCIPLES' SECTIONS REMOVED AND GENERAL UPDATE	Jon Bowker	Peter De Leo	Digitally signed by Peter De Leo DN: cn=Peter De Leo, c=AU, email=peter.deleo@lycopodium.com Date: 2025.05.15 13:47:47 +0800
2	25.09.24	REVISED AS NOTED (previously HRM-POL-002)	MB	PDL	25.09.24
1	14.10.15	REVISED AS NOTED	-	PDL	14.10.15
0	14.03.07	ISSUED FOR USE	SR	RLL	26.03.07
REV NO.	ISSUE DATE	DESCRIPTION OF REVISION	BY	APPROVED	Lycopodium Limited Board APPROVED

## Table of Contents

	<i>Page</i>
<b>1.0 POLICY</b>	<b>1</b>
<b>2.0 COMPLIANCE WITH AUSTRALIAN PRIVACY PRINCIPLES</b>	<b>1</b>
2.1 Collection of Personal Information	2
2.2 Disclosure of Personal Information and Security	2
2.3 Accuracy of Personal Information	3
2.4 Openness	4
2.5 Identifiers	4
2.6 Cross-Border Transmission of Personal Information	4
<b>3.0 EXEMPTION FROM THE AUSTRALIAN PRIVACY PRINCIPLES - EMPLOYEES</b>	<b>4</b>
<b>4.0 DEFINITIONS</b>	<b>4</b>

## 1.0 POLICY

Lycopodium is committed to ensuring individual privacy in the way it collects, stores, uses and disposes of personal information. Lycopodium is also bound by the Australian Privacy Principles as incorporated in the Privacy Act 1988 (Cth). The Australian Privacy Principles can be viewed here [Australian Privacy Principles](#). In addition, by reason of its international operations and/or the locations in which Lycopodium subsidiaries conduct business, Lycopodium is also bound by the privacy laws pertaining to each of the various jurisdictions in which it operates.

This policy sets out the obligations and procedures that Lycopodium personnel must comply with when they encounter or are involved in the collection or dissemination of Personal Information or Sensitive Information. The policy applies to Personal Information and Sensitive Information pertaining to any person, including without limitation, employees, officers, contractors, subcontractors, clients and members of the public. To the extent any applicable legislation imposes privacy obligations that are more onerous or protective than the obligations in this policy, then the more onerous or protective obligation will prevail.

This policy applies to all employees of Lycopodium and persons working for Lycopodium under a contract or a consultancy agreement.

## 2.0 COMPLIANCE WITH AUSTRALIAN PRIVACY PRINCIPLES

The Privacy Act obligates Lycopodium and all its personnel to comply with the Australian Privacy Principles. In simple terms, the Australian Privacy Principles seek to address:

- Open and transparent management of personal information (APP 1).
- Anonymity and pseudonymity (APP 2).
- Collection of solicited personal information (APP 3).
- Dealing with unsolicited personal information (APP 4).
- Notification of the collection of personal information (APP 5).
- Use or disclosure of personal information (APP 6).
- Direct marketing (APP 7).
- Cross-border disclosure of personal information (APP 8).
- Adoption, use or disclosure of government related identifiers (APP 9).
- Quality of personal information (APP 10).
- Security of personal information (APP 11).

- Access to personal information (APP 12).
- Correction of personal information (APP 13).

Notwithstanding the existence of privacy laws in other jurisdictions, the Australian Privacy Principles are one of the more detailed and comprehensive sets of privacy principles and are strongly aligned with other privacy laws.

## **2.1 Collection of Personal Information**

Lycopodium can collect Personal Information from any individual subject to the following limitations and conditions. Where the individual is not an employee, then the information can only be collected if it is reasonably necessary to the functions or activities of Lycopodium and certain conditions are complied with.

- The individual must be made aware that Personal Information is being collected.
- The individual is given contact details for the Lycopodium person who is responsible for collecting that Personal Information.
- The individual is informed of how the Personal Information will be used, is informed that they have a right of access to the Personal Information and informed of consequences (if any) if they refuse to provide Personal Information.

Lycopodium must ensure that Personal Information is collected in a fair and lawful way and if reasonable or practical, collect it directly from the individual concerned.

Lycopodium should not collect Sensitive Information pertaining to any individual. The only exceptions, where Sensitive Information can be collected, are:

- Where the Sensitive Information pertains to an employee and directly pertains to the employment relationship (including past employment relationship).
- Where collection of that information is required by law (this will be very unusual where the individual is not an employee).
- Where collection of that information is necessary to prevent serious or imminent threat to the health or safety of any person.

## **2.2 Disclosure of Personal Information and Security**

All Lycopodium personnel must maintain strict security and confidentiality over any Personal Information and Sensitive Information which they are entrusted with. If personnel are provided with such information which they do not believe they require access to, they must immediately inform the disclosing party and return the Personal Information.

Further, Lycopodium personnel must not disclose Personal Information to any party (including other personnel) except in the following cases:

- Where the Personal Information pertains to an existing or former employee, then the information can be used and disclosed for any purposes that are related to the current or former employment relationship.
- For any other Personal Information, disclosure is only allowed for the purposes for which that Personal Information was originally collected (or for a reasonably related purpose).
- Where the individual to whom the Personal Information pertains has given written consent for disclosure.

Sensitive Information shall not be disclosed to anyone except where it is necessary to prevent serious or imminent threat to health or security, or where the individual to whom the information pertains has given written consent for disclosure.

All Personal Information and Sensitive Information must be stored in a secure location where access is restricted only to those personnel who have a need to access that information.

When information is no longer required to be stored, it should be destroyed or permanently de-identified.

## **2.3 Accuracy of Personal Information**

All Lycopodium personnel who are involved in the collection, usage or disclosure of Personal Information have an obligation to take reasonable steps to make sure that information is accurate, complete and current. In most cases, it is not possible to confirm whether data provided by an individual is accurate, other than to ask for confirmation of accuracy. However, if any person gives notice that Personal Information is not accurate, then the person responsible for the collection of that Personal Information must be informed, must investigate the allegation, must record in writing the results of that investigation, and, if the information is inaccurate, correct the inaccuracy.

In addition, any person (including third parties) has a right to access their Personal Information (but not any information relating to another person) and also to seek correction of any inaccuracies in their Personal Information. Where a person requests access to information, or seeks correction of an inaccuracy, that person's request must be forwarded to the person responsible for the collection and storage of that information ('Information Recipient'). The Information Recipient must then consider the request for access or investigate the allegation of inaccuracy. If there are possible reasons why the person's request should be rejected, the Information Recipient must report their concerns to the Chief Financial Officer (CFO) or Group Financial Controller. There are various grounds for which a request for access to information may be denied, as specified in the Australian Privacy Principles. A response which denies a person a right of access to Personal Information should be in writing and include the reasons for denial. This response should be reviewed by the CFO prior to issue.

## 2.4 Openness

Any person (including third parties) may access a copy of Lycopodium's Privacy Policy, which is publicly available on the Company's website and internally on the Company's intranet.

## 2.5 Identifiers

As specified within the Australian Privacy Principles, an organisation must not adopt a government related identifier (for example, a tax file number, driver's license number or passport number) of an individual as its own identifier of the individual, unless an exception applies. Records should be stored according to an individual's name or other internal Lycopodium identification system instead.

## 2.6 Cross-Border Transmission of Personal Information

For Personal Information pertaining to persons other than Lycopodium employees, that Personal Information shall not be sent overseas, unless that individual consents to the international transmission, or otherwise where there is certainty that the recipient will be subject to an obligation of confidence and non-disclosure with respect to that Personal Information. For employees, such information may be transferred where it is necessary as part of the employment relationship.

## 3.0 EXEMPTION FROM THE AUSTRALIAN PRIVACY PRINCIPLES - EMPLOYEES

Note: there is an exception to the obligation to comply with the Australian Privacy Principles to the extent any act or practice in relation to Personal Information is directly related to the current or former employment relationship. The exemption only applies to Personal Information generated or obtained by the employer in the course of the person's employment and only applies to the employer's use of the information. Any third parties that are provided with the employee's Personal Information (for example a client) must comply with the Privacy Principles and Lycopodium has a limited obligation to ensure that third party intends to comply with the Privacy Principles (usually this is achieved by obtaining confirmation from the third party that it shall maintain confidentiality and comply with privacy laws).

The exemption does not apply to contractors or subcontractors, nor does it apply to Personal Information obtained during the recruitment process. Accordingly, in those situations, the Australian Privacy Principles must be complied with. Further, it does not apply to Sensitive Information.

## 4.0 DEFINITIONS

**Employee** – an individual employed on a full-time or part time, and continuing basis, including 'salaried' employees, casual employees and personnel engaged via a registered agency or payroll provider, or their own company (referred to as contractors).

**Information Recipient** – person responsible for the collection and storage of information.

**Lycopodium or the Company** – Lycopodium Limited including any of its subsidiaries or other controlled entities, excluding joint ventures.

**Personal Information** – information, including government identifiers, or an opinion (whether true or not and whether recorded in material form or not), about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

**Sensitive Information** – information or an opinion about an individual's race, ethnic origin, political opinions, political affiliation, religion, philosophical belief, professional or trade association memberships, trade union membership, sexual preference, criminal record or health information.

**Note:** Capital and lower-case letters, singular and plural have the same meaning in the application of the definitions within this policy.