

Privacy Policy

HRM-POL-L-034

Uncontrolled if printed

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>
1.0 POLICY	1
2.0 SCOPE	1
3.0 DEFINITIONS	1
4.0 COMPLIANCE WITH NATIONAL PRIVACY PRINCIPLES	1
4.1 Collection of Personal Information	2
4.2 Disclosure of Personal Information and Security	2
4.3 Accuracy of Personal Information	3
4.4 Openness	3
4.5 Identifiers	4
4.6 Cross-Border Transmission of Personal Information	4
5.0 EXEMPTION FROM THE NATIONAL PRIVACY PRINCIPLES - EMPLOYEES	4

1.0 POLICY

Lycopodium **Limited** (Lycopodium **Minerals**) is committed to ensuring individual privacy in the way it collects, stores, uses and disposes of personal information. Lycopodium is also bound by the National Privacy Principles as incorporated into the Privacy Act 1988 (Cth). A copy of the National Privacy Principles is reproduced at the end of this Policy. [2]

2.0 SCOPE

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.

3.0 DEFINITIONS

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

'Sensitive Information' means 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.

4.0 COMPLIANCE WITH NATIONAL PRIVACY PRINCIPLES

The Privacy Act obligates Lycopodium and all its personnel to comply with the National Privacy Principles. The full text of the National Privacy Principles is reproduced at the end of this Policy. In simple terms, the National Privacy Principles seek to:

- regulate the collection, use and disclosure of Personal Information (NPP 1 and 2)
- set out obligations to maintain the accuracy and completeness of information collected and stored, including a right of an individual to seek correction of information (NPP 3 and 6)
- maintain security over collected information (NPP 4)
- inform individuals (both employees and third parties) about Lycopodium's privacy and information collection policies (NPP 5)
- give individuals access to Personal Information stored about them (NPP 6)
- refrain from identifying individuals based on identifiers assigned by a government body (for example, a tax file number) (NPP 7)

- give third parties the option of maintaining anonymity when entering into transactions with Lycopodium (NPP 8)
- regulate transfer of Personal Information across borders (NPP 9), and
- refrain from collecting Sensitive Information or disclosing it except in very restricted circumstances (NPP 10).

4.1 Collection of Personal Information

Lycopodium can collect Personal Information from any individual. 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 information will be used, is informed that they have a right of access to the 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); or where collection of that information is required by law (this will be very unusual where the individual is not an employee); or where collection of that information is necessary to prevent serious or imminent threat to the health of any person.

4.2 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 information.

Further, Lycopodium personnel must not disclose Personal Information to any party (including other personnel) except in either of 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 information was originally collected (or for a reasonably related purpose).
- Where the individual to whom the 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 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.

4.3 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 up-to-date. 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, which are contained in NPP6.1. A response which denies a person a right of access to information should be in writing and give the reasons for denial. This response should be reviewed by the CFO prior to issue.

4.4 Openness

Any person (including third parties) may request a copy of Lycopodium's Privacy Policy. Such requests should be forwarded to the Chief Financial Officer or Group Financial Controller. The Privacy Officer shall then be responsible for ensuring that person is given the latest copy of the Privacy Policy.

4.5 Identifiers

No Lycopodium personnel shall keep any records of any person where those records identify an individual based on an identifier assigned by a government body (for example, a tax file number, driver's license number or passport number). Records should be stored according to an individual's name or other internal Lycopodium identification system instead.

4.6 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 information. For employees, such information may be transferred where it is necessary as part of the employment relationship.

5.0 EXEMPTION FROM THE NATIONAL PRIVACY PRINCIPLES - EMPLOYEES

Note: there is an exception to the obligation to comply with the National Privacy Principles to the extent any act or omission 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 information obtained during the recruitment process. Accordingly, in those situations, the National Privacy Principles must be complied with. Further, it does not apply to Sensitive Information.

NATIONAL PRIVACY PRINCIPLES

1.0 COLLECTION

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
- a) the identity of the organisation and how to contact it
 - b) the fact that he or she is able to gain access to the information
 - c) the purposes for which the information is collected
 - d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind
 - e) any law that requires the particular information to be collected
 - f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.
- 1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in this section except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2.0 USE AND DISCLOSURE

- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:
- a) both of the following apply:
 - i) The secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection
 - ii) The individual would reasonably expect the organisation to use or disclose the information for the secondary purpose, or

-
- b) the individual has consented to the use or disclosure, or
 - c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - i) it is impracticable for the organisation to seek the individual's consent before that particular use, and
 - ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications, and
 - iii) the individual has not made a request to the organisation not to receive direct marketing communications, and
 - iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications, and
 - v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically, or
 - d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
 - i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure, and
 - ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph, and
 - iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information, or
 - e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
 - i) a serious and imminent threat to an individual's life, health or safety, or

-
- ii) a serious threat to public health or public safety, or
 - f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or
 - g) the use or disclosure is required or authorised by or under law, or
 - h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
 - i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law
 - ii) the enforcement of laws relating to the confiscation of the proceeds of crime
 - iii) the protection of the public revenue
 - iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct
 - v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in Subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose

of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite Subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

- a) the individual:
 - i) is physically or legally incapable of giving consent to the disclosure, or
 - ii) physically cannot communicate consent to the disclosure, and
- b) a natural person (the carer) providing the health service for the organisation is satisfied that either:
 - i) the disclosure is necessary to provide appropriate care or treatment of the individual, or
 - ii) the disclosure is made for compassionate reasons, and
- c) the disclosure is not contrary to any wish:
 - i) expressed by the individual before the individual became unable to give or communicate consent, and
 - ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware, and
- d) The disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of Subclause 2.4, a person is **responsible** for an individual if the person is:

- a) a parent of the individual, or
- b) a child or sibling of the individual and at least 18 years old, or
- c) a spouse or de facto spouse of the individual, or
- d) a relative of the individual, at least 18 years old and a member of the individual's household, or
- e) a guardian of the individual, or
- f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health, or

- g) a person who has an intimate personal relationship with the individual, or
- h) a person nominated by the individual to be contacted in case of emergency.

2.6 In Subclause 2.5:

- a) **Child** of an individual includes an adopted child, a step-child and a foster-child, of the individual.
- b) **Parent** of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.
- c) **Relative** of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.
- d) **Sibling** of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3.0 DATA QUALITY

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4.0 DATA SECURITY

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5.0 OPENNESS

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6.0 ACCESS AND CORRECTION

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

-
- a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual, or
 - b) in the case of health information—providing access would pose a serious threat to the life or health of any individual, or
 - c) providing access would have an unreasonable impact upon the privacy of other individuals, or
 - d) the request for access is frivolous or vexatious, or
 - e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings, or
 - f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations, or
 - g) providing access would be unlawful, or
 - h) denying access is required or authorised by or under law, or
 - i) providing access would be likely to prejudice an investigation of possible unlawful activity, or
 - j) providing access would be likely to prejudice:
 - i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law, or
 - ii) the enforcement of laws relating to the confiscation of the proceeds of crime, or
 - iii) the protection of the public revenue, or
 - iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct, or
 - v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders,
 - vi) by or on behalf of an enforcement body, or

- k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches Subclause 6.1 if it relies on Subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where Subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

- a) must not be excessive, and
- b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7.0 IDENTIFIERS

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- a) an agency, or
- b) an agent of an agency acting in its capacity as agent, or
- c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, Subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in Subclause 7.1, unless:

- a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency, or
- b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure, or
- c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an **identifier**.

8.0 ANONYMITY

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9.0 TRANSBORDER DATA FLOWS

9.1 An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles, or
- b) the individual consents to the transfer, or
- c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or
- d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or
- e) all of the following apply:
 - i) the transfer is for the benefit of the individual
 - ii) it is impracticable to obtain the consent of the individual to that transfer
 - iii) if it were practicable to obtain such consent, the individual would be likely to give it, or
- f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10.0 SENSITIVE INFORMATION

10.1 An organisation must not collect sensitive information about an individual unless:

- a) the individual has consented, or
- b) the collection is required by law, or
- c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - i) is physically or legally incapable of giving consent to the collection, or
 - ii) physically cannot communicate consent to the collection, or

- d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities
 - ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent, or
- e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite Subclause 10.1, an organisation may collect health information about an individual if:

- a) the information is necessary to provide a health service to the individual, and
- b) the information is collected:
 - i) as required by law (other than this Act), or
 - ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite Subclause 10.1, an organisation may collect health information about an individual if:

- a) the collection is necessary for any of the following purposes:
 - i) research relevant to public health or public safety
 - ii) the compilation or analysis of statistics relevant to public health or public safety
 - iii) the management, funding or monitoring of a health service, and

- b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained, and
- c) it is impracticable for the organisation to seek the individual's consent to the collection, and
- d) the information is collected:
 - i) as required by law (other than this Act), or
 - ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
 - iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with Subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.