



COMPANY POLICY

Privacy

LIT-POL-047

Month Year Jul-24 Revision Code Rev 0 Approved by Board of Directors

Controlled Document Approved for Distribution

Revision Code	Revision Date	Name	Position	Signature	Next Review Date
Rev 0	03-Jul-24	Board	Board	Board	03-Jul-26

1. INTRODUCTION

Protecting privacy is very important to Lithium Australia. This policy sets out how the Group collects and processes your personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles. It also sets out your rights in relation to the personal information the Group holds about you.

2. PURPOSE

This policy describes how the Group deals with personal identifiable information of individuals that it interacts with – this includes its employees, representatives of its suppliers, customers, sponsors and business partners, landowners, industry association representatives, users of the Group website and mobile applications, shareholders and job applicants.

3. DEFINITIONS

Table 3-1 Definitions

Term	Definition
The Group	Lithium Australia Limited (ACN 126 129 413) and its subsidiaries
Privacy Act 1988 (Cth)	Australian legislation enacted to safeguard the privacy of individuals and regulate the handling of personal information by Australian Government agencies and organisations in the private sector. It sets out the Australian Privacy Principles (APPs), which outline standards for the collection, use, disclosure, and storage of personal information.
OAIC	Office of the Australian Information Commissioner is an independent agency within the Australian Government's Attorney-General's portfolio. Its primary functions are privacy, freedom of information and government information policy.
Personal Identifiable Information	Means any information about an identified or identifiable person. This includes where you can be identified, directly or indirectly, including by reference to an identifier (for example, a name or email address, or an online identifier such as a unique device identification number). The words "process" and "processing" are used to describe the various things the Group may do with your personal information – including using, disclosing, holding, recording, storing, transferring or otherwise handling that information.
Sensitive Personal Identifiable Information	Means information that is more private than others (which, depending on jurisdiction, includes information about someone's racial or ethnic origin, political opinions, religious beliefs or affiliations, health or medical conditions, genetic information, biometric information, sexual orientation, criminal record, trade-union membership and political association membership).

4. RESPONSIBILITIES

Table 4-1 Responsibility matrix

Role	Responsible
Board	Promote the establishment privacy policies and procedures. Ensure compliance with privacy laws and regulations. Provide oversight and allocate resources for privacy protection measures.
Managing Director/ Chief Executive Officer	Establish internal control systems and procedures including regular auditing to ensure that they are effective in minimising the risk of non-compliance with this policy
People and Culture	Manage employee personal identifiable information. Train employees on this policy Handle employee inquiries and concerns regarding their information
Payroll (Finance)	Manage employee records in accordance with privacy laws.
Managers/Supervisors	Provide regular and appropriate training on how to comply with this policy to relevant personnel
Employees/contractors /volunteers/visitors	Required to understand and comply with this policy

5. TYPES OF PERSONAL INFORMATION COLLECTED

Different types of personal identifiable information are collected and processed depending on how you interact with the Group. In some cases, this may include information that shows who you are and/or is linked to you because of your interactions with the Group. In some circumstances, this may include the collection of sensitive personal information about you.

5.1 How personal identifiable information is collected

Personal identifiable information is primarily collected from you either directly (such as in the normal course of business, as an employee, when you subscribe to a news alert or request information from the Group, including through the Contact Us form or Online Booking available on the website) or indirectly from your interactions with the Group (such as by monitoring your use of the Group's website). In some cases, personal identifiable information may also be collected about you from third parties (such as recruitment agencies).

5.2 Types of personal identifiable information collected

The types of personal identifiable information that may be collected about you includes:

- Identification data – such as your name, gender, job title, photograph and date of birth.
- Contact details – such as your home and business address, email address and telephone number.
- Recruitment-related information – such as your name, email address, location, telephone number, qualifications, employment history, interests, types of roles you are interested in, your work application form and resume or CV. If you progress through the interview process, additional information such as interview notes, references, results of any psychometric tests and background checks (including criminal records checks), your work visa and other information to verify your identity and right to work may also be collected.
- e-Business information – this includes information required to provide access to the Groups e-Business website page (such as login information, IP addresses), and records of your use of this website.
- Usage information – information such as server log information (your IP address, browser type, operating system, browser language, time zone, access times and any referring addresses) and location information.
- Other information – this includes information about access and attendance to the Group's premises and physical assets (such as security records about times of entry and exit, and information collected through CCTV), details about your use of the Group's assets, communications with you (including complaints or concerns raised by you or any feedback or survey responses that you provide) and other information you voluntarily provide to the Group.

5.3 Sensitive Personal Identifiable Information

At times sensitive personal identifiable information may be collected about you (such as health or medical information, criminal history checks, or your racial or ethnic origin), but this will only occur as described as follows.

The Group processes personal identifiable information to conduct its business – this includes managing contractual relationships, recruitment, monitoring access to websites and apps, managing safety and security risks, and complying with its legal obligations. Sensitive personal identifiable information is also processed where you have provided your consent, or it is necessary to comply with legal obligations.

The purposes for which your personal identifiable information is processed will depend on the type of personal identifiable information collected and the context in which it was collected. However, the primary purposes for which personal identifiable information is processed includes:

- Managing the Group's relationship with you – this includes providing you with information or services, improving Group products and services and communicating with you;
- Business-related purposes – this includes negotiating, managing, and fulfilling Group contracts with customers, suppliers and third parties (including e-commerce transactions), managing business relationships, administering real estate leases and licences, conducting clearance procedures, managing accounts and records, supporting corporate social responsibility activities, resource planning and workforce management, activities and operations, internal investigations, and debt administration;
- Marketing purposes – this includes analysing the characteristics of website visitors; to prepare analytics and profiling for business intelligence purposes; to personalise website experience; managing newsletters and communications and, where the Group collects details in the membership database relevant to the Group's customers for demographic analysis;

- Recruitment-related purposes – this includes considering you for career opportunities with the Group and inviting you to participate in recruitment activities and events;
- Managing safety and security risks – this includes managing and monitoring safety, security and access to the Group's sites (including through the use of CCTV);
- Managing the Group's IT resources (including monitoring electronic communications);
- Website administration and internal operations – this includes troubleshooting, data analysis, testing, research, statistical and survey purposes;
- Managing shareholder relationships – this includes for the purposes of undertaking share transactions, dividend payments and communications with shareholders; and
- Legal obligations – this includes meeting obligations imposed under law, responding to lawful requests from governments and public authorities, and responding to potential or actual litigation.

Personal identifiable information may also be collected for any other purposes for which you have provided your consent or if there is another lawful basis for doing so.

Sensitive personal identifiable information about you will only be collected and processed:

- Where you have explicitly provided your consent; or
- Where otherwise permitted by applicable laws and regulations; and
- In accordance with the Group's Employee Records Policy (LIT-POL-044).

5.4 Consent Process

When the Group requires the collection of sensitive personal identifiable information, it will ask you for this consent, which is voluntarily, meaning you have a genuine choice and control over whether or not to provide your sensitive personal identifiable information. Additionally, consent will be specific to the information being collected and the purposes for its use. If you choose not to provide your consent, it may however prevent the Group from advancing your interest in its business activities.

The Group will maintain a detailed written record of when and how your consent was obtained, including the information provided to you at the time and your response.

You have the right to withdraw your consent at any time. Where sensitive personal identifiable information has been provided for a job application, you can do this by emailing this request to hr@lithium-au.com. For all other requests through the Contact Us form or emailing this request to info@lithium-au.com. Once consent is withdrawn, the Group will cease using your sensitive personal identifiable information for the purposes for which consent was given and will not rely on any past consent for any future use or disclosure of this information. Your sensitive personal identifiable information will be deleted unless there is a legal requirement to retain it.

5.5 Cookies

The Group's websites and apps may use cookies. Cookies are small pieces of data stored on the web browser of your device. These are used for site administration and analysis purposes and to deliver tailored content. If you wish not to take advantage of cookies, you may configure your browser not to accept them (although this may disable or render unusable some of the features on the website).

5.6 Hyperlinks

While the Group's website may contain links to other websites, you are encouraged to read the privacy policies of those websites before providing your personal information as they may differ substantially. The Group is not responsible for the privacy practices or the content of these other websites.

6. SHARING YOUR PERSONAL INFORMATION

The Group may share your personal identifiable information internally as well as with third parties involved in the running of the Group's business and your authorised representatives. This may involve sharing information across national borders. The Group ensures that any transfer of personal identifiable information overseas complies with Australian Privacy Principle Number 8, cross-border disclosure of personal information. This involves confirming that the overseas recipient is governed by laws or binding schemes that provide protections equivalent to the Australian Privacy Principles or obtaining explicit consent for the transfer.

6.1 Disclosures within the corporate group

Your personal identifiable information (which may sometimes include sensitive personal identifiable information) may be shared within the corporate group who require the information for the purposes detailed in this policy. This may include sharing your personal identifiable information with Group entities in countries other than where the information was originally collected.

6.2 Disclosures outside the corporate group

Sharing your personal identifiable information (which may sometimes include sensitive personal identifiable information) may be required with:

- People you have authorised to interact with the Group on your behalf (such as recruitment agencies);
- Third parties who provide business services to the Group (such as external HR, IT and security service providers);
- Prospective purchasers of all or part of Group's business or of any shares in Lithium Australia;
- The Group's professional advisors (such lawyers and accountants); and
- Government authorities or other persons when obliged to do so by an applicable law.

If there is a need to disclose personal information to third parties in a different country to where the information was collected, the Group will take steps to ensure that there is a lawful basis for the disclosure and that the disclosure complies with all applicable laws. This may include entering a legally binding contract with the recipient under which they are obliged to handle your information in accordance with applicable laws.

7. STORING AND PROTECTING YOUR PERSONAL INFORMATION

The Group takes steps to ensure that your personal identifiable information is kept secure and protected against unauthorised access or use. Personal identifiable information is only kept for as long as it is needed to carry out the purposes described in this policy.

In the event of a data breach, the Group will follow the procedures outlined by the Notifiable Data Breaches scheme, including assessing the breach, notifying affected individuals and the Office of the Australian Information Commissioner if required, and taking steps to mitigate any harm.

7.1 Information security

The Group has put in place procedures and technologies to maintain the security of your personal identifiable information.

Steps have also been taken to ensure that all Group workers are aware of, and are properly trained through applicable information security policies and procedures that are designed to keep your personal identifiable information secure. The Group will investigate and take appropriate action if it becomes aware of any failure to comply with these policies and procedures.

7.2 Storing personal identifiable information

Personal identifiable information that is collected is generally stored in electronic databases. These databases are hosted in the Group's fileserver in Brisbane, and third party data centre in Australia.

Third parties may also be utilised to store and process your personal identifiable information. However, this will only happen if the party agrees to comply with the Group's procedures and policies or if they put in place equivalent security measures.

7.3 Information retention

Personal identifiable information will only be kept for the purposes described in this policy or as otherwise required by law.

7.4 Job applicants

Personal identifiable information for unsuccessful job applicants **may be retained for 12 months** for the purposes of considering you for other roles within the Group. However, the Group is under no obligation to retain your

personal information for this purpose and may elect to delete your personal information at any time following an unsuccessful application.

You may request to have your personal identifiable information deleted from the Group's database at any time. You can do this by emailing this request to hr@lithium-au.com.

8. YOUR RIGHTS AND CHOICES

You have rights relating to your personal identifiable information held by the Group. Let us know if you want to correct your personal identifiable information or if you have concerns about how the Group is handling your personal identifiable information.

You have certain rights in relation to your personal identifiable information that the Group holds about you, though the details of these may vary depending on the country where you are based. The Group will respond to all requests received from individuals wishing to exercise their rights in relation to any information that is held in accordance with applicable data protection laws.

If you wish to access, correct or update any personal identifiable information that is held about you, please lodge a request in the Contact us form available on the website. It is important that all of the information the Group holds about you is correct and up-to-date.

If you are concerned about how the Group is dealing with your personal identifiable information, then you may have the right to complain to an applicable data protection authority. The relevant authority will depend on which country you are located. For Australia, complaints can be made to the Office of the Australian Information Commissioner.

Before raising a complaint with a data protection authority, it is recommended that you first raise the issue with the Group so it can be addressed as quickly as possible. The Group will make a record of your complaint and will deal with it as quickly as it can while keeping you informed of progress. Even if the Group is not able to address your concern, it will be able to provide further information about how you can contact a relevant data protection authority.

8.1 Country-specific rules

Additional privacy rules and restrictions relating to the Group's management of your personal identifiable information may apply in some countries where the Group operates.

The Group will only process your personal identifiable information where it has a legal basis for doing so. This means it will process your personal identifiable information:

- Where necessary in connection with the entry into or performance of a contract between you and the Group;
- To comply with the Group's legal obligations;
- Where it is in the Group's legitimate business interests; or
- Where you are given a genuine choice as to whether the Group collects your data and you have given your consent. Where you have consented, you will always have the option to withdraw this consent at a later stage.

8.2 Your Rights

In addition to the rights set out above, you have the right, in certain circumstances, to request:

- The erasure of any personal information that the Group holds about you;
- The restriction of processing of any personal identifiable information that the Group holds about you; and
- The transfer of your personal identifiable information from the Group to a third party.

You also have the right to object to the processing of your personal identifiable information by the Group in certain circumstances.

8.3 Regular Audits and Training

The Group conducts regular audits to ensure compliance with privacy policies and provides ongoing training to employees on privacy and data collection.

9. POLICY REVIEW

The Board will review this policy from time to time where necessary to reflect changes in the Group's privacy compliance practices. The Board must approve any amendments made to the policy as a result of any review and will update this policy as required or as a result of new laws or regulations.

10. REFERENCES

LIT-POL-011 (Information Technology) policy

LIT-POL-044 (Employee Records) policy