Privacy Policy
Torrens Mining Limited
ACN 168 295 092

1. Introduction

At Torrens Mining Limited (**Company**) (together with entities the Company controls, the **Group**) we recognise the importance of protecting the privacy and the rights of individuals. This Privacy Policy has been published to provide a clear outline of how and when personal information and other date is collected, disclosed, used, stored and otherwise handles by the Company.

We take privacy seriously and we will only collect and use your personal information as outlined below.

Our Privacy Policy fully complies with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Policy Principles (**APPs**) as at 11 February 2021.

2. Collection of Personal Information

The Group only collects personal information if it is necessary for our business purposes. The information we collect will depend on the purpose for which it is collected. It may be limited to contact details where we interact with the public (e.g. through a website) or it may include more detailed information where a client, employee or shareholder relationship exists.

3. Use of Personal information

We generally use personal information for the primary purpose for which it is collected. That may include supplying our services or responding to an individual's request.

Depending on the purpose for which we have collected personal information, we may store some of the information in our company records. Some or all of this information may be available to partners and authorised staff of the Group for use in accordance with this policy.

Internally, we have controls and procedures to ensure that personal information provided to us remains confidential. All of our staff are trained in privacy and are bound by strict duties of confidentiality to the Group and its clients.

We will not collect or use personal information in ways other than as stated in this policy unless we have obtained an individual's consent. In some cases we may specifically request a consent form to be signed. In other cases, consent may be implied (for instance, where an individual gives us information after being fully advised of how it will be used).

4. Types of personal information which may be collected

The types of personal information we may collect depends on the purpose for which it has been collected, but may include your name, address, email address, telephone number, purchasing preferences and history, and financial details, among other things. We will only collect personal information that is needed in connection with the provision of our products and services to you.

We may also collect sensitive information about you (for example health information) where:

(a) you consent;

(b) the collection is required by law or for insurance purposes;

(c) the collection is necessary for your health and safety; and/or

(d) the collection is to establish, exercise or defend a legal or equitable claim.

As appropriate, we will notify you of the collection of your personal information and tell you why we are collecting personal information and how we plan to use it, or these things will be obvious when we collect the information.

No matter how we collect your personal information we will not seek to make any unreasonably intrusive enquiries of you or as to this information.

5. Disclosure of Personal Information

We do not sell or trade personal information, or allow third parties to use that personal information for their own purposes.

If information needs to be accessed by a third party, we attempt to limit that access to the extent necessary for the third party to provide services to us or to perform its functions. We will ensure, to the fullest extent possible, that those suppliers and contractors are also bound by duties of confidentiality, and by the same privacy obligations as the Group itself.

In all other cases, we will only disclose personal information to a third party if the disclosure is permitted by law (including under the Australian Privacy Principles).

We will not disclose personal information to overseas recipients.

We also ask our clients to confirm that they have made their own disclosures or obtained consents before they pass any personal information to us.

6. Accessing and updating your personal information

We will provide access to personal information upon request by an individual, unless a request is unreasonable and the Australian Privacy Principles would permit us to decline that access (for instance, where granting access would infringe another person's privacy).

Individuals who wish to gain access to their personal information should contact the Privacy Officer using the contact details set out in our website.

When you make a request to access personal information, we will require you to provide some form of identification (e.g. driver's licence or passport) so we can verify that you are the person to whom the information relates. In some cases, we may also request an administrative fee to cover the cost of access.

7. Data Breach Reporting

7.1 What is an eligible data breach?

An eligible data breach is either:

(a) Unauthorised access or disclosure of information that a reasonable person would conclude is likely to result in serious harm to any individuals to whom the information relates; or

(b) Information that is lost in circumstances where unauthorised access or disclosure of information is likely to occur and it can be reasonably concluded that such an outcome would result in serious harm to any of the individuals to whom the information relates.

Serious harm can include identity theft, and serious physical, psychological, emotional, financial or reputational harm.

7.2 Company Response Plan

When a data breach has occurred or is suspected to have occurred, the Company Secretary (acting as the Privacy Officer) will initiate the following process:

(a) When an employee or contractor becomes aware or suspects that there has been a data breach, they will immediately notify their manager who will assess the risk, document the incident and report to the Privacy Officer.

(b) The Privacy Officer will include details of breach into data breach register and report to Board if the data breach may reasonably constitute an eligible data breach to determine a response.

(c) If the Board decides that there are reasonable grounds to suspect an eligible data breach it must initiate the Reporting process in Paragraph 7.4. This assessment must occur within 30 days of first notification in clause (a).

(d) Depending on the seriousness of the breach the Board may appoint a staff member or response team comprising personnel with the necessary expertise to respond.

(e) The staff member or response team must take immediate steps to contain the breach including:

(i) Stopping practice causing breach;

(ii) Recovering information;

(iii) Shutting down systems;

(iv) Changing computer privileges;

(v) Addressing electronic security weaknesses; and

(vi) Alerting building security.

However, it should be noted that there is no single method of responding to a data breach and in some cases the following steps may need to be modified. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

7.3 Record Keeping

The response team or staff member appointed to respond to the breach must ensure evidence is preserved that may be valuable in determining the cause of the breach and keep appropriate records of the suspected breach including what steps have been taken to rectify the situation and the decisions made.

The assessment form in Schedule 1, must be completed by the Board upon notification of a suspected breach.

7.4 Reporting of Breaches

If the Company becomes aware that there are reasonable grounds to believe that there has been an eligible data breach as under the Privacy Act, the Company will:

(a) Prepare a statement that sets out:

(i) the identity and contact details of the entity;

(ii) a description of the eligible date breach that the entity has reasonable grounds to believe has happened;

(iii) the kind or kinds of information concerned; and

(iv) recommendations about the steps that individuals should take in response to the eligible data breach

(b) Give a copy of the statement in (a) to the Privacy Commissioner.

The steps in (a) and (b) must be done as soon as practicable after the Company becomes so aware of the eligible data breach.

The Company will then:

(a) If practicable notify each individual to whom the relevant information relates of the contents of the statement in (a) or take such reasonable steps to do so;

(b) If practicable notify each individual at risk from the eligible data breach of the contents of the statement in (a) or take such reasonable steps to do so;

(c) If neither (a) or (b) can be practicably achieved, publish a copy of the statement on the Company's website or take reasonable steps to publicise the contents of the statement.

7.5 Review

After the incident, the eligible data breach will be reviewed by the Privacy Officer and any actions determined necessary to prevent future breaches implemented.

8. Complaints

If you believe that the information we hold about you is incorrect, or if you have concerns about how we are handling your personal information we ask that you contact us and we will try to resolve those concerns.

All complaints should be initially in writing and directed to the Privacy Officer at:

Privacy Officer
Torrens Mining Limited
Level 11, 216 St Georges Terrace
Perth WA 6000
Email: info@torrensmining.com

We will respond to your complaint within 30 days and try to resolve it within 90 days. If we are unable to resolve your complaint within this time, or you are unhappy with the outcome, you can contact the Office of Australian Information Commissioner via its enquiries line 1300 363 992 or website http://www.oaic.gov.au/ to lodge a complaint.

9. Updates to this policy

This Privacy Policy may be amended from time to time. Whenever you need to refer to this policy you should contact us or check our website for the most up to date version.

Changes to this Privacy Policy will not affect our use of previously provided personal information.

Schedule 1- Data Breach Assessment Report

Description	Details
Description of Breach	
Type of Information involved	
How was the breach discovered	
How the breach was discovered	
Cause and extent of breach	
List of affected individuals	
Is the breach likely to result in serious harm to any of the individuals to whom the harm relates?	
Remedial action	
Is or will remedial action result in making serious harm no longer likely?	
Who will be notified of the breach?	
Preliminary recommendations	
Name of response team members	
Date	