DATA PROTECTION & PRIVACY POLICY
Predictive Discovery Ltd (ACN 127 171 877)

1. Introduction

This Data Protection & Privacy Policy (the "**Policy**") outlines the principles, standards, and procedures adopted by Predictive Discovery Limited ("**Predictive**" or the "**Company**") to ensure the lawful and secure handling of personal and sensitive information. Our commitment is to maintain strict compliance with applicable laws and protect the privacy and rights of employees, shareholders, and other stakeholders.

2. scope

This Policy applies to Predictive Discovery as the ultimate holding company and to all its subsidiaries, affiliates, operations, systems, and personnel worldwide. All subsidiaries are required to comply with this Policy in addition to any applicable local data protection, privacy, or cybersecurity laws and regulations in the jurisdictions in which they are incorporated or operate.

This Policy establishes a **minimum group-wide standard**. Where local laws or regulations impose more stringent requirements, those local requirements shall prevail.

3. Regulatory Framework and Jurisdictional Coverage

Without limitation, the Company operates in accordance with:

- the Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles;
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy legislation;
- applicable data protection, privacy, cybersecurity and record-keeping laws in all jurisdictions in which the Company operates; and
- internationally recognised best practices observed by ASX- and TSX-listed mining companies.

The Company continuously monitors legislative and regulatory developments and updates its practices accordingly.

4. Definitions

Personal Information means any information relating to an identified or identifiable individual, including employee, shareholder, contractor, community member or other stakeholder information.

Sensitive Information includes information subject to enhanced legal protection, such as health, biometric, financial, identification or similar data, where applicable under law.

5. Lawful Collection and Use of Personal Information

The Company collects and processes personal information only where:

- it is necessary for legitimate business purposes, including employment administration, shareholder relations, regulatory compliance, health and safety, security, community engagement and operational management;
- there is a lawful basis under applicable law (including consent where required); and

- the collection is fair, transparent and limited to what is reasonably necessary for the stated purpose.

Personal information is not used for secondary purposes incompatible with the original purpose of collection unless permitted or required by law.

6. Transparency and Notices

The Company provides clear and appropriate privacy notices to individuals, informing them of:

- the types of personal information collected;
- the purposes of collection and use;
- potential disclosures (including cross-border transfers);
- their rights under applicable privacy laws; and
- how to contact the Company regarding privacy matters.

7. Data Security and Cybersecurity

The Company implements appropriate technical, organisational and administrative measures to protect personal information against loss, misuse, unauthorised access, alteration or disclosure, including:

- access controls and authentication measures;
- cybersecurity risk assessments and monitoring;
- employee training and awareness programs;
- incident detection, response and escalation procedures; and
- secure information systems and data storage practices.

Security measures are proportionate to the sensitivity, volume and risk associated with the information.

8. Data Breach Management

The Company maintains procedures for identifying, managing and responding to data breaches. Where required by law, affected individuals and regulators will be notified in a timely manner.

All actual or suspected data breaches must be reported immediately in accordance with internal incident response protocols.

9. Employee Personal Information

Employee personal information is collected, used and disclosed strictly for legitimate employment and operational purposes. Access is limited to authorised personnel on a need-to-know basis.

Employees are informed of their rights under applicable laws, including rights of access, correction and complaint. Personal information is retained only for as long as required by law or legitimate business needs and is securely destroyed thereafter.

10. Shareholder and Investor Information

Shareholder and investor personal information is handled with the highest degree of confidentiality and care. Disclosure is limited to:

- compliance with corporate, securities and regulatory obligations;
- engagement of service providers (such as share registries) under appropriate safeguards; or
- circumstances otherwise permitted or required by law.

11. Third-Party Service Providers

Where personal information is disclosed to third parties (including contractors, advisors, IT providers or service partners), the Company:

- conducts reasonable due diligence;
- requires contractual commitments to maintain appropriate privacy and security standards; and
- monitors compliance where practicable.

Third parties may only use personal information for authorised purposes.

12. Cross-Border Data Transfers

Personal information may be transferred across borders where necessary for business operations. In such cases, the Company takes reasonable steps to ensure that transferred information receives a level of protection comparable to that required under applicable privacy laws.

13. Data Subject Rights

Subject to applicable laws, individuals have the right to:

- request access to their personal information;
- request correction of inaccurate or incomplete information;
- withdraw consent where applicable; and
- lodge complaints regarding the handling of personal information.

Requests are handled in a timely, transparent and lawful manner.

14. Governance and Accountability

Overall responsibility for this Policy rests with senior management. Day-to-day oversight is delegated to a designated privacy or data protection function.

All employees and relevant third parties are required to comply with this Policy. Breaches may result in disciplinary action and contractual consequences.

15. Training and Awareness

The Company provides appropriate training and guidance to employees and relevant personnel to ensure awareness of privacy obligations and secure data handling practices.

16. Records Retention

Personal information is retained only for as long as required to fulfil its purpose or to comply with legal, regulatory or operational requirements. Secure disposal procedures apply at the end of retention periods.

17. Policy Review and Updates

This Policy is reviewed at least annually and whenever material changes occur in legislation, regulatory expectations or Company operations.

Material amendments are communicated to relevant stakeholders as appropriate.

Date Approved	**2026-05-27**
Owner	Board of Directors