Redpath Mining Inc. – Global Privacy Policy

Policy name	Global Privacy Policy
Date published	June 2026
Version	3.0
Owner	Chief Compliance Officer

This Global Privacy Policy ("Policy") is a public statement that explains how the Redpath Group ("Redpath Group", "Redpath", "we", "our" or "us") collects, uses, processes, manages, and discloses personal data in connection with the activities covered by this Policy. It also outlines how we apply data protection principles in connection with our external website and other external interactions involving website visitors, including, but not limited to, job applicants and clients purchasing products or services. This Policy applies to all such personal data, but does not cover personal data of Redpath employees, contractors, and internal users, which is addressed in Redpath's Employee Privacy Policy and related internal notices, where applicable. By publishing the Policy on our external website, the Redpath Group provides transparency regarding the personal data we collect, use, process, manage, and disclose.

This Policy also covers personal data collected through Redpath's other dealings with external individuals, whether or not the information is collected through its website, except where a separate Redpath privacy notice applies.

Where required by law, Redpath will inform website visitors of the purposes of which the cookies are used and will obtain their prior, informed consent for the use of all cookie categories before such cookies are activated. Redpath may require a separate Cookie Policy for the use of Google Analytics (Reference: https://www.termsfeed.com/blog/cookies-policy-google-analytics/)

Introduction

The Redpath Group is committed to protecting your privacy. This Policy describes how and why we collect, use, process, manage, and disclose individuals' personal data, and provides information about individuals' rights in relation to their personal data. We may use personal data provided to us for any of the purposes described in the relevant sections of this Policy or as otherwise communicated at the point of collection.

Please review this Policy carefully. By submitting your personal data to us, registering for or using our services, accessing our website, or otherwise voluntarily interacting with us, you acknowledge that Redpath may may collect, use, process, manage, and disclose your personal data as described in this Policy and subject to applicable law, which may be updated from time to time.

What Does the Redpath Group Consider Personal Data?

Personal data is any data which is related to an identified or identifiable natural person. The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. Furthermore, personal data may also include technical and security-related information associated with the use of our website, systems, or communications channels where that information relates to an identified or identifiable natural person.

What Kind of Personal Data Does Redpath Collect?

We may collect personal data when you contact or communicate with us by phone, mail, e-mail or via our website.

When you access, visit or use our website, we may collect the following information using the following tools:

- your email address, account credentials or authentication information, your curriculum vitae and any other information you disclose to us when you register to build a profile to apply for jobs;
- your email , account credentials, authentication information, and access records when you log on to access your account;
- your name, phone number, region of residence, email address and any other information you provide to us when you contact us through an online form for a specific project;
- your technical and device information when you visit our website may be automatically collected. Such information may include your internet protocol address, information about your device, browser and operating system, and the date and time of your visit; and
- your information necessary to authenticate you, manage access to certain services, record user preferences, document acknowledgements or consents where required, and to protect our systems and communications against phishing, fraud, malware, unauthorized access, and similar cybersecurity threats.

Where sign-in, access control, acknowledgement, authorization, preference

management, or consent management is required for certain digital services, we may use enterprise identity and access management solutions. Such solutions may be cloud-based and may be used by Redpath to authenticate users, manage access permissions, and record access decisions, authorizations, acknowledgements, preferences, and, where applicable, consent choices associated with access to Redpath systems or services.

We may also use enterprise data governance, security, and compliance tools. These tools support Redpath in classifying, protecting, retaining, auditing, and managing personal data and other information processed through Redpath systems in accordance with legal, regulatory, and business requirements. Where applicable to the activities covered by this Policy, such tools may be used to support data protection, records management and retention, audit logging, regulatory compliance, as well as incident response. Employee and contractor personal data processed through such tools is addressed in Redpath's Employee Privacy Policy and related internal notices.

In addition, Redpath may use AI-assisted cybersecurity tools, including email security tools, to analyze communications sent to, received from, or processed through Redpath systems or services, together with related metadata, headers, links, attachments, and security signals for the strictly limited purpose of identifying, preventing, investigating, and mitigating phishing, spam, malware, account compromise, fraud, and similar cybersecurity risks. Such tools are used to protect Redpath, its systems, information assets, website visitors, applicants, customers, suppliers, service users, and other persons who communicate with Redpath, and are not deployed for general monitoring of communications unrelated to cybersecurity.

What are the Purposes for the Collection, Use, Processing, Management and Disclosure of Your Personal Data?

The Redpath Group may collect, use, process, manage, and disclose your personal data for the following reasons:

- to apply for a job or request a service or product. Applicable legal basis under the European Union General Data Protection Regulation ("GDPR"): steps prior to entering into a contract, performance of a contract, legitimate interests, consent where applicable, or compliance with legal obligations;
- for recruitment purposes. Applicable legal basis under GDPR: steps prior to entering into a contract, performance of a contract, legitimate interests, consent where applicable, or compliance with legal obligations;
- to complete a service or facilitate the purchase of a product: Applicable legal basis under GDPR: performance of a contract or service;

- to respond to inquiries or requests related to a service or a product, or to support one-time or ongoing communications with the Redpath Group: Applicable legal basis under GDPR: performance of a contract or a service;
- authenticate, authorize users and manage access to digital services and systems. Applicable legal basis under GDPR: legitimate interest of the Redpath Group;
- record and manage access decisions, authorizations, acknowledgements, preferences, and, where applicable, consent choices records captured through authentication and access-management tools, including enterprise identity and access management solutions used by Redpath. Applicable legal basis under GDPR: legitimate interest of the Redpath Group;
- classify, protect, retain, audit, investigate, and govern personal data and other information processed through Redpath systems using where applicable to the activities covered by this Policy. Applicable legal basis under GDPR: legitimate interest of the Redpath Group;
- detect, prevent, investigate, and respond to phishing, email fraud, spam, malware, malicious links or attachments, unauthorized access, account compromise, suspicious activity, or other security events using automated and AI-assisted cybersecurity and email security technologies, where applicable to the activities covered by this Policy. Applicable legal basis under GDPR: legitimate interest of the Redpath Group and, where applicable, compliance with legal obligations;
- maintain and retain audit trails, logs, and records relating to the activities covered by this Policy where reasonably necessary to demonstrate compliance with legal, regulatory, contractual, and internal governance obligations. Applicable legal basis under GDPR: legitimate interest of the Redpath Group and, where applicable, compliance with legal obligations;
- to monitor and enhance the security of Redpath's physical premises and assets. Applicable legal basis under GDPR: legitimate interests of the Redpath Group;
- protect Redpath's systems, website visitors, applicants, customers, suppliers, service users, and other persons who communicate with Redpath, information assets, and business operations in connection with the activities covered by this Policy through proportionate technical and organizational security controls. Applicable legal basis under GDPR: legitimate interest of the Redpath Group and, where applicable, compliance with legal obligations; and
- other purposes for which we have obtained your consent, and for such other purposes as may be permitted or required by applicable law.

Redpath will, where required by applicable law, rely on an appropriate legal basis for these activities, including consent, performance of a contract, steps prior to entering into a contract, compliance with legal obligations, and/or Redpath's legitimate interests in

maintaining the security, integrity, compliance, and lawful operation of its website, systems, services, communications, and business operations.

Access decisions, authorizations, acknowledgements, preferences, and, where applicable, consent choices captured through Redpath access-management processes, including enterprise identity and access management solutions where applicable, may be recorded by Redpath, including he fact, date, time, method, and relevant record of that access decision, authorization, acknowledgement, preference, or consent choice for compliance, audit, and evidentiary purposes.

If processing is based on your consent, you may withdraw that consent at any time by contacting us using the details provided in the "Contacting Us About Your Privacy" section of this Policy, subject to our retention policies and legal obligations and any other lawful basis Redpath may have to continue processing the personal data. In some cases, withdrawal of your consent may result in the Redpath Group being unable to provide you with a particular service or product (including but not limited to customer support for sales and consideration of a job application).

Who Does the Redpath Group Share Your Personal Data With?

The Redpath Group may share your personal data with third parties to assist in administering activities on our website (such as maintenance), with our auditors or other professional advisors, or in connection with service-related communications and activities. The Redpath Group may also share personal data with service providers to assist with hosting, maintaining, securing, analyzing, and improving our website, systems, services, and communications. If you have provided the Redpath Group with your personal data, that personal data will not be sold.

Where applicable, Redpath may also disclose personal data to service providers or other third parties in connection with the promotion of its services, subject to applicable law and any required consent.

More specifically, when we engage service providers who process personal data on our behalf or provide services to us, we will share your personal data with such service providers subject to contractual or other appropriate requirements that such personal data is processed only for the purposes of providing services to Redpath or as otherwise permitted by applicable law. For example, we may engage service providers (i) to support or outsource the processing of website, system, service, communication, security, and data-governance functions such as hosting, infrastructure, and storage services; or (ii) to analyze the performance and use of our website.

If we provide your information to service providers, we require those service providers to

maintain appropriate confidentiality, security, privacy, and data protection safeguards for your personal data. When our service providers no longer need your personal data for these limited purposes, we require that they securely delete, return, anonymize, or otherwise dispose of such personal data, as appropriate and in accordance with applicable contractual and legal requirements. In some circumstances, we may permit our service providers to retain aggregated, anonymized or statistical information that does not identify you. We do not authorize the service providers to disclose your personal data to unauthorized parties or to use your personal data for their own direct marketing purposes. If you would like more information about our service providers, please contact us using the details provided in the “Contacting Us About Your Privacy” section of this Policy.

Redpath may also share personal data with providers of security, identity and access management, hosting, infrastructure, analytics, governance, compliance, and cybersecurity services, including providers that support authentication, access control, audit logging, data classification, records management, retention, eDiscovery, legal hold, data loss prevention, and cybersecurity monitoring. Such providers may include providers of identity and access management services, data governance and compliance tools, hosting, infrastructure, storage, website analytics, and automated and AI-assisted email security, cybersecurity monitoring, and threat-detection services.

In connection with AI-assisted cybersecurity or email security tools, Redpath and its service providers may process communications sent to, received from, or processed through Redpath systems or services, including email content, metadata, headers, attachments, links, sender-recipient relationship signals, security signals, and similar information, including through automated analysis of behavioral patterns and anomalies, solely for the limited purpose of detecting, preventing, investigating and responding to suspected phishing, spam, malware, account compromise, fraud, unauthorized access, malicious activity, or other cybersecurity risks, and not for general surveillance or monitoring of communications unrelated to cybersecurity. For greater clarity, Redpath personnel do not routinely access or review the contents of ordinary communications for general monitoring, personal, or surveillance purposes.

Any human review by Redpath is limited to authorized personnel and to circumstances where review is reasonably necessary, including where communications have been specifically flagged, quarantined, escalated, or otherwise identified through applicable security processes as potentially malicious, suspicious, unauthorized, or requiring investigation. Moreover, any access by our service providers’ personnel is subject to contractual confidentiality, security, privacy, and data protection restrictions. Such access is limited to reviewing information that has been flagged, quarantined, escalated,

or otherwise identified by the service provider's software or security processes as potentially malicious, suspicious, unauthorized, or requiring investigation, and only to the extent reasonably necessary to provide services, maintain the security of the service, troubleshoot issues, or comply with legal and regulatory obligations.

Additionally, we may use and disclose your personal data where we reasonably believe such use or disclosure is permitted by applicable law, necessary or appropriate, including:

- to comply with applicable law, including laws outside your country of residence;
- to comply with legal process;
- to respond to requests from public authorities and government bodies, including those outside your country of residence;
- to enforce the terms of our agreements for products and services;
- to protect our operations or those of our affiliates or subsidiaries;
- to protect our rights, privacy, safety or property, or those of our affiliates, you or others;
- to enable us to pursue available remedies or limit damages; and
- to a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our business, brands, affiliates, subsidiaries or other assets.

If we intend to disclose your personal data to a new category of third party, we will identify the relevant category of third party or recipient and the purpose of the disclosure and provide notice or obtain consent where required by applicable law.

Where is Your Personal Data Located?

Your personal data may be stored and processed in any country where we have facilities or in which we engage third party service providers, such as Canada, the United States of America, South Africa and the European Union. As a result, your personal data may be transferred to countries outside your country, state, or province of residence, which may have different data protection rules than those that apply in your place of residence. While your personal data is located outside of your jurisdiction, it will be subject to the laws of the jurisdiction in which it is processed, and may be disclosed to governments, courts or law enforcement or regulatory authorities in accordance with those laws.

We will ensure that appropriate safeguards are in place to protect your personal data in accordance with applicable legal requirements, and that our processing of your personal data remains governed by this Policy and applicable laws at all times. Where service providers supporting identity and access management, compliance, governance,

hosting, infrastructure, data protection, cybersecurity, email security, or threat-detection functions process personal data on Redpath's behalf, such processing may occur in jurisdictions in which those providers or their subprocessors operate, subject to applicable law and appropriate contractual, organizational, technical, and transfer safeguards.

Additional information regarding the transfers described above and the corresponding safeguards implemented by the Redpath Group is available by contacting us using the details provided in the "Contacting Us About Your Privacy" section of this Policy.

Does the Redpath Group Use Cookies?

The Redpath Group uses cookies and other tracking technologies to collect and analyze statistics relating to this website. Cookies are small data files transferred to your computer's hard-drive by a website. They keep a record of your preferences, making your subsequent visits to the site more efficient. We may also use them, with your consent, to identify you for purposes such as managing your preferences, other purposes described in our Cookie Policy. Data used for analytics may be processed by an organization external to the Redpath Group. Examples of tracking include the number and frequency of visits, the average length of visits and which pages are viewed during a visit as well as the types of browsers and the Internet Protocol Addresses of visitors' computers.

Cookies or similar technologies may be stored locally on mobile devices or on computer servers operated or controlled by our third-party service providers. In addition, when you visit our website, our systems automatically collect your IP address and the type of browser that you use. We may use third party service providers to support analytics, advertising, or similar website related services, where permitted by applicable law and, where required, with your consent. The use of cookies or other similar technologies by such third parties is governed by their privacy policies. You may limit the automatic collection of certain information on our website through the cookie preference tools made available on our website or through your browser settings, where applicable. Please be aware that disabling cookies may prevent you from using specific features on our website. We may use cookies and log files to track user information. For more information, please refer to the Cookies Policy [Link to the Cookies Policy to be inserted].

How Long Does the Redpath Group Retain Your Data?

The Redpath Group is subject to a wide range of laws governing its business. To meet these obligations, the Redpath Group implements regional Data Retention Policies and retains personal data as required to comply with applicable regional legal requirements.

Such data is retained only for as long as the relevant legal obligation remains in effect or there is another valid business purpose for its retention. Once personal data is no longer required, the Redpath Group securely disposes of it in accordance with its Data Retention Policy and applicable local legislation.

Security, access, authentication, authorization, acknowledgement, consent where applicable, audit, cybersecurity, and data-governance records may be retained for longer periods where reasonably necessary to investigate incidents, respond to cybersecurity events, demonstrate compliance, protect legal rights, maintain business continuity, or comply with legal, regulatory, or contractual obligations.

Data Subject Rights

You may request details of the personal data that we hold about you. If you would like a copy of your personal data, please contact us using the details provided in the "Contacting Us About Your Privacy" section of this Policy. If you believe that any personal data we hold about you is inaccurate or incomplete, please contact us as soon as possible. We will promptly correct or update such personal data.

In certain circumstances, you may have additional rights, including the following:

- the right to withdraw consent to processing where processing is based on consent;
- the right to object to the unlawful processing of personal data, under certain conditions;
- the right to have your personal data erased or deleted, subject to certain conditions;
- the right to request a restriction of the processing of personal data, under certain conditions, for example, if you believe that the Redpath Group has exceeded the legitimate basis for the processing, that the processing is no longer necessary, or that the personal data is inaccurate;
- the right to data portability or transferability of personal data in a structured, commonly used and machine-readable format, under certain conditions; and
- the right to object to decisions made by automated means that have legal effect on you or similarly affect you significantly, under certain conditions.

To exercise any of these rights, please contact us using the details provided in the "Contacting Us About Your Privacy" section of this Policy.

The Redpath Group is entitled to refuse access to your personal data in certain situations as provided by Applicable Privacy Laws.

Where Redpath uses automated or AI-assisted tools for cybersecurity, email security, fraud prevention, identity and access management, data governance, compliance, audit, records-management, or incident-response purposes, such tools are used to

support security, compliance, access management, data protection, and risk management functions. Redpath will handle requests concerning such processing in accordance with applicable privacy laws, while also taking into account Redpath's security obligations, confidentiality obligations, legal privilege, investigation requirements, legal restrictions, and the rights and freedoms of others.

If you have any complaints regarding the Redpath Group's privacy practices, you may have the right to lodge a complaint with the appropriate national data protection authority.

How Does the Redpath Group Protect your Personal Data?

The Redpath Group is committed to ensuring that your personal data is secure. In order to prevent unauthorized access or disclosure, we have put in place appropriate technical and organizational measures to safeguard and secure the personal data we process. We have also taken steps to ensure that the only personnel who are granted access to your personal data are those with a business 'need-to-know' or whose duties reasonably require such information. The Redpath Group exercises care in the secure transmission of your personal data when transmitting personal data across borders or to third party systems or service providers; however, no transmission of data over the Internet is completely secure. The Redpath Group cannot guarantee that data disclosed through the Internet cannot be intercepted by malicious third parties. However, the Redpath Group has taken the steps that are reasonably available to the Redpath Group to protect any personal data that you have provided to us, including when such personal data is disposed of, deleted, anonymized, returned, or destroyed. These measures may include identity and access controls, authentication and authorization technologies, security monitoring, audit logging, data loss prevention, records management, legal hold, eDiscovery, data retention controls, encryption, incident response procedures, phishing detection, email security, threat detection, and other data protection and cybersecurity safeguards, including tools provided by third-party service providers and enterprise technology platforms supporting Redpath's security and compliance program. Where Redpath uses automated and AI-assisted cybersecurity and email security technologies, those technologies are implemented as part of Redpath's broader cybersecurity program and are intended to identify, prevent, investigate, and respond to malicious, suspicious, or unauthorized activity, not to create unnecessary access to personal data or to enable indiscriminate human review of ordinary communications.

If, despite all our reasonable efforts, a data breach does occur, the Redpath Group will take appropriate steps to contain, investigate, and mitigate the impact of the breach. In the event of a data breach that is likely to result in a high risk to individuals rights and freedoms, Redpath will notify affected individuals, where required by applicable law, and

provide information regarding steps that may be taken to reduce potential harm. Redpath will notify the relevant supervisory authorities without undue delay, in accordance with applicable legal requirements.

Contacting Us About Your Privacy

If you have questions, concerns, or requests regarding this Policy or the Redpath Group's privacy practices, please contact our Chief Compliance Officer and Privacy Officer at: privacy@redpathmining.com.

We may update this Policy from time to time where appropriate, including to reflect changes in applicable laws, regulations, or our data processing practices.

Policy History/Revision Dates

Origination Date: June 2021
Last Amended Date: June 2026
Next Review Date: June 2027