Computer Usage and Conduct Policy

This Computer Usage and Conduct Policy establishes guidelines for the correct use of company email, internet and telecommunication resources by employees, directors and officers of Gateway Mining Limited (**Company**) and all its related bodies corporate.

All employees, directors and officers of the Company have the responsibility to use Internet, email and telecommunication resources in a professional, ethical and lawful manner. As with the Company's other resources, its computer and telecommunications systems belong to the company and should only be used for authorised, work-related business purposes.

1. Mobile Telephones

Due to the nature of their work, some employees may be eligible to have a Company mobile phone as part of their position. Alternatively, an employee may be reimbursed for the cost of business related phone calls made from an employee's personal mobile phone where the employee is not provided with a company mobile phone. Employees are expected to adhere to the following:

- return any messages or missed calls promptly;
- ensure their mobile phone is charged at all times;
- maintain their mobile phone in good working order;
- make every reasonable effort to ensure that any company supplied mobile phone (if applicable) is secure at all times, this includes ensuring it is not left unattended out of the workplace or in a vehicle

In the event that an allocated mobile phone is lost or stolen, the employee is to contact their supervisor and if unavailable any senior member of the Company as soon as is practicable and liaise with the relevant personnel they are instructed to contact. This is likely to enable the Company to suspend the sim card and take appropriate steps to safeguard the Company's IT Infrastructure and confidential information.

Employees must take due care when using Company supplied phones and take reasonable steps to ensure that no damage is caused. Employees must report any damage to their manager who will determine the action to be taken.

An employee may be held responsible for any costs incurred if he or she has not taken due care of the allocated mobile phone. If an employee negligently or repeatedly damages or loses a mobile phone a second-hand phone may be issued or alternatively, the privilege be withdrawn (at the discretion of the Company).

Employees may be asked to justify monthly bills. The Company reserves the right to make the appropriate deductions from payroll for any amounts in excess of the monthly threshold. Employees may be asked to justify specific single call charges or text messages on the monthly bill.

2. The Internet

Due to its global nature, users of the Internet may encounter material that is inappropriate, offensive and, in many instances, illegal. The Company cannot control the availability of this information and it is difficult to restrict access to all of it. However, all employees are notified that they are responsible for any material which they:

- view on the internet
- download from the internet
- upload to the internet

Although employees may access the internet for personal use, it is important to remember that the Company's IT Support can and will monitor usage of such resources. Please refer to the compliance section of this policy for further details.

Use of electronic mail and internet is not an automatic right by way of employment at the Company. Use of electronic mail or internet may be revoked for a user or group of users at any time.

3. Prohibited Uses

Employees may not use the Company's Internet resources for commercial or personal advertisements, solicitation, promotions, destructive programs (such as viruses), political material or any other unauthorised or personal use.

4. Prohibited Activities

Sending, receiving, displaying, printing or otherwise disseminating material, which is fraudulent, harassing, illegal, sexually explicit, obscene, intimidating or defamatory is prohibited. Employees encountering such material should report it to their supervisor immediately. Harassment laws (and other anti-discrimination laws) at both Commonwealth and State level can deem the individual responsible for any breaches of anti-discrimination legislation. Harassment, bullying and anti-discrimination policies apply to all use of the computer system.

Never download or transmit:

- rude, lewd, pornographic or any other material which may be offensive to others;
- chain mail or any mail that may be interpreted as a form of harassment;
- junk or random mail;
- material containing illegal content;
- material that is or is potentially discriminatory, defamatory, sexual or offensive.

5. Accessing the Internet

Employees may only access the Internet on their own computers unless otherwise agreed with their supervisor.

6. Social Media

The Company expects all its employees to behave in an appropriate and acceptable professional manner.

Employees are required to use any social media site with the same level of professionalism they would demonstrate in a corporate meeting, phone call or email. Employees should be aware that the employee's opinion when expressed on a social network site could have a detrimental effect on the profitability or reputation of the Company. If it is found that such commentary has or is likely to have an adverse impact on the business or its associates, disciplinary action will be taken.

Employees must always use social networking sites in a lawful manner including all laws relating to harassment, equal opportunity and privacy.

Any communication on social networking sites must be conducted in line with the responsibilities in any of the Company's charters and policies.

6.1. Usage

Employees are to limit access to social networking sites using Company or personal resources during working hours. Should the aforementioned limited access lead to a distraction of an employee's work then the employee's manager or management of the Company may determine that no access to social networking sites using Company or personal resources during workings hours should be conducted and that any access shall be restricted to rest break periods only away from their desks.

6.2. Content

Employees who access social media sites whether by Company or personal resources must not post comments or images relating to the Company or its colleagues, contractors, work functions, or other employees without express written permission to do so.

Any employee failing to adhere to this requirement will be managed in accordance with the Company's disciplinary procedures.

Employees are reminded that they are bound contractually to act in good faith and have a duty of fidelity to the employer not to harm the business or damage the reputation of the Company and the people associated with it.

6.3. Confidential Information

Employees by common law have duties to the Company to not knowingly misuse, or wrongfully disclose the Company's confidential information during employment. Employees may also have appropriate restraints in their employment contract to protect the business if the employee was to leave the Company's employment for any reason. Any breach of these post-employment restrictions may result in legal action. Employees should refer to their employment contract for clauses relating to confidential information and/or restraints and ensure they abide by these clauses.

7. Email

The Company recognises that private use of email can sometimes be necessary. Employees should be mindful that the personal use of email is a privilege and should be limited in both number and duration.

Employees are also reminded that although access to email services is often password protected, this does not mean that it is restricted from access by the Company's IT Support along with the management of the Company. Refer to the Compliance section of this policy for further information of monitoring of email and internet access and usage.

7.1. Communicating Information

Employees are expected to exercise the same care in drafting email messages they would for any other form of written communication. Any messages on the Company's computer system may be subject to

review by authorised personnel. Furthermore, email messages or social media postings may be produced as evidence in a litigious matter involving the Company.

No email shall contain foul language, derogatory or defamatory comments, or anything that would not be contained in a normal business communication or memo. (This includes jokes, sound files and video clips).

Generation or dissemination of chain letters and widespread dissemination (mailing multiple addresses) of unrelated business material is prohibited.

Employees are reminded that sending an email that contains personal information about another person, may breach privacy laws if it is not used for the purpose for which it was collected.

- Employees should not send an email that does not identify them as the sender;
- Employees will not use another employees log on or user id to send an email;
- Emails received in error must be notified to the sender immediately and then deleted. It must not be copied to any other party;
- It is not considered good manners to use CAPITAL LETTERS other than for headings or emphasis. It is looked upon as shouting;
- The use of emoticons should be limited to informal email correspondence only.

7.2. Security and retention

- Do not send confidential information to parties other than the intended recipient and do not breach copyright.
- Do not send non-internal documents by open email as the contents may be easily copied, reprinted, reproduced or circulated etc. Use Adobe Acrobat or similar software and send a 'read only' / 'pdf' version.
- Keep incoming, outgoing and sent emails for 24 months before archiving.

8. Cloud Security

Employees must:

- only access Company data on the cloud if they have been granted explicit authorisation. Access must be limited to the data necessary to perform their job functions.
- use multi-factor authentication (MFA) if the Company requires when accessing company data on the cloud to enhance security.
- use strong, unique passwords for accessing cloud services and must not share their passwords with others.
- ensure that any data transmitted to or from the cloud is encrypted to protect against unauthorised access.
- participate in training sessions as required by the Company on cloud security, data protection, and compliance with relevant legislation.

9. Defamation

It is unlawful to be a party to or to participate in the trafficking of any defamatory message. To defame someone, defamatory material, including words or matter, must be published which is or is likely to cause

an ordinary, reasonable member of the community to think less of the defamed person (the plaintiff), or to injure the plaintiff in his or her trade, credit or reputation.

For the purpose of defamation law, 'publication' is very broad and includes any means whatsoever that is used for communication, including electronic messaging. A message containing defamatory material made electronically is, by its very distribution, 'published'. A message containing defamatory material is also published if it is simply received electronically and forwarded on electronically. Employees should be aware that the Company is at risk of being sued for any defamatory material stored, reproduced or transmitted via any of its facilities.

10. Copyright

Not all information on the Internet is in the public domain or freely available for use without proper regard to rules of copyright. Much of the information is subject to copyright protection under Australian law and, by Australia's signature to international treaties, also protected at international levels. 'Use' includes downloading, reproducing, transmitting or in any way duplicating all or part of any information (text, graphics, videos, cartoons, images or music) which is not in the public domain.

11. Virus Detection

All material downloaded from the Internet or from computers or networks that do not belong to the Company **must** be scanned for viruses (and other destructive programs) before being placed onto the Company's computer network, as per the Company's Cyber Security Policy (GML_COR_017_POL). A failure to comply with this requirement will seriously jeopardise its computer systems. The Company strictly prohibits downloading of any information for personal use onto its computer network.

Be aware of any attachment with email from unsolicited or unknown sources. Do not open any suspicious attachments without running virus protection and checking with Company's IT provider.

No personal software or data is to be downloaded onto Company equipment without prior specific consent of the employee's suprevisor.

Ensure you regularly run our virus protection programmes in conjunction with our IT provider.

12. Waiver of Privacy

The Company has the right to monitor any and all aspects of its computer system including, but not limited to, monitoring any internet sites visited or accessed by staff, monitoring chat groups and news groups, reviewing material downloaded or uploaded by staff and reviewing email messages sent and received by staff. Subject to any applicable telecommunications and privacy laws, employees waive any rights to privacy that they may have in respect of anything that they create, store, send, or receive on or through the Company's computer and telecommunications system.

Where an employee works part-time, is on annual leave, personal leave or any other leave, the Company's management or others as directed, will, if necessary, access the employee's email and computer system to ensure the Company provides a continuous service as expected by its clients.

13. Compliance with Applicable Laws and Licenses

Employees are required to comply at all times with all software licenses, copyrights and any other applicable legislation (including, but not limited to, intellectual property and telecommunications laws). Where directed by a lawful authority, the Company will provide all logs of internet usage, email correspondence and content of emails.

14. Compliance

All employees and consultants who use the Company's computer and telecommunications resources are required to comply with this Policy at all stages during their employment. Improper use of Company resources (i.e. phone, email and internet) may result in a threat to system security; the privacy of staff and others; and the liability of the organisation. As such, a failure to comply with the Policy may result in disciplinary action, including, in serious circumstances, dismissal or termination of the consultancy agreement.

A review of each employee's compliance with this policy may be conducted annually or at any other time as required. The review will be undertaken by Company Management and/or the Company's IT providers.