



# PANORAMIC RESOURCES LIMITED

ACN 095 792 288

---

## Information Technology Management Policy

---

**Policy No: 1**

**Title**                      **Group Internet and Email Policy**

### **Purpose**

Panoramic Resources Limited (PRL) is committed to ensuring all employees understand their obligations and responsibilities when using Company internet and email facilities. This Policy is designed to ensure all users are aware of the PRL conditions concerning connection to, and the use of, Internet services via Company information resources. The Policy will also cover the PRL email service and the conditions concerning its use as a means of correspondence with both internal and external parties.

### **Scope**

This document details the email and Internet acceptable use policies to be followed by PRL employees. All levels of management are required to actively support its implementation.

This Policy applies to all staff, contractors and consultants employed by PRL and its subsidiaries, who use PRL Perth Office or site email and Internet services. It covers the following:

- Internal use of email;
- Remote use of email; and
- Email sent and received via external networks such as the Internet.

## Objectives

The objectives of this Policy are to:

- Increase understanding of the requirements for the use and management of email, the Internet and Intranet in PRL.
- Reduce corporate exposure from inappropriate email and Internet practices, computer viruses, malicious software and to ensure compliance with legal requirements.
- Increase understanding by employees that their actions may have legal implications and could adversely affect them, if they act outside the Policy guidelines.
- Promote acceptable use of email and the Internet in PRL resulting in benefits such as:
  - Enhanced customer services.
  - Improved ability to store and recover critical information.
  - Reduced corporate risk from inappropriate email and Internet practices.

## Effective Date

3 September 2008

## Access

After a staff member or contractor has completed induction, a computer logon and email account will be assigned. The electronic mailbox and Internet must be used in accordance with this Policy. The content, maintenance and use of an electronic mailbox are the responsibility of the person to whom the email account is assigned.

## Internet Acceptable and Prohibited Use

Internet services are provided by PRL to support open communications and exchange of information. PRL encourages the use of electronic communications by its employees.

While the Internet contains much information that is useful for work purposes, it also contains significant volumes of information that may be interesting, but which is of limited direct use to the activities of PRL. All employees should endeavour to maximise the value of their time on the Internet and avoid the unnecessary time and cost of 'surfing the net' when such activities add little value to work.

It is permissible to use the Internet for incidental personal purposes such as banking, paying bills and booking flights and accommodation. This does not include uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate Group Policy with regard to employee time commitments or Company equipment.

- Limited personal use does not include downloading:
  - unauthorised software;
  - lengthy files containing picture images;
  - live pictures or graphics;
  - computer games;
  - music files;
  - the accessing of radio or television stations broadcasting via the Internet (streaming);
  - accessing FaceBook or MySpace (or similar interactive websites); and
  - chat channels.

Downloading of such files increases the load on the network and could degrade the service to other staff with a genuine business need to use the Internet. Such files are not to be emailed to others.

The Internet contains some information that is offensive. This includes hate mail, racist and pornographic material. All intentional access to such material is prohibited.

### **Subscription to Lists**

Subscription to list servers is to be kept to those that relate to the Group's activities - subscription to lists that are not work related is not permitted. In order to ensure a manageable level of emails received, which will not interfere with normal work obligations, it is advisable to limit the amount of lists to which you subscribe. Subscribing to email lists can increase the chances of spam - ensure reasonable effort is taken to understanding the conditions to which your email address may be subjected to and that your email address cannot be used by third parties.

### **Restriction on Sites that can be Visited**

PRL may monitor usage of the Internet by employees, including reviewing a list of websites accessed by an individual. No individual should have any expectation of privacy in terms of their usage of the Internet. In addition, PRL will restrict access to certain sites that it deems are not necessary for work related purposes. These include sites that contain illegal, obscene, pornographic or hateful content, which is objectionable or inappropriate in the workplace.

## Downloading

Software should not be downloaded from the Internet without prior approval of the IT Manager. Downloaded software can introduce computer viruses onto PRL's network. In addition, anti-virus download software is not to be disabled or bypassed. All computers are configured to automatically scan any material downloaded from the Internet.

## Email Acceptable and Prohibited Use

Use of email throughout the Group network infrastructure is permitted where such use is required for business purposes, effective internal/external communications and supports the goals and objectives of the Group and its business units. Employees are not to use email for:

- Illegal or unethical purposes.
- Distributing threatening, abusive, defamatory, prohibited or offensive messages.
- The practice of harassment, abuse or defamation of any person.
- Distributing chain letters, SPAM or unnecessary multiple messages.
- Making false representation or breaching confidentiality.
- Unauthorised use or release of Company information.
- The distributing and/or knowingly receiving of unauthorised software.
- Potentially embarrassing or negative impacts on the Company.

**Ephemeral emails referring to non-business matters** (e.g. social events, footy tipping) should be utilised on a limited basis. These should be discarded after use to ensure system and network resources are not impeded. The content, maintenance and use of an electronic mailbox are the responsibility of the person to whom the email account is assigned.

Categories of behaviour and email deemed to be unacceptable are:

- Networking of jokes with derogatory content and images of an offensive nature.
- Posting sexual innuendos or personal information about others.
- Sending messages that spread rumours about another employee.
- Passing on material containing threats or violent fantasies.

Computer work stations and the services accessible on them are provided to employees for business use to carry out tasks related to work. Services include email and the Internet. Reasonable private use of email and the Internet is permitted. However, it must be noted that this is a privilege and, as such, use needs to be balanced in terms of the Group's commitment to the development of a responsive and flexible workplace and operational needs. Every employee has a responsibility to be ethical and efficient in their official or private use of public property and services and to be productive in the use of their work time.

It is not acceptable to intentionally create, send or access information that could damage the Company's reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory. Inappropriate use includes, but is not limited to, any use of Company equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.

You may be individually liable if you aid and assist others who discriminate against, harass or vilify colleagues or any member of the public. (Harassment will be treated in accordance with the Company's existing grievance handling procedures and may result in disciplinary action and/or termination of employment).

You may not intentionally create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws. The Company reserves the right to audit and remove any illegal material from its computer resources without notice.

Email is not to be intentionally used for chain letters. Employees are encouraged to report breaches of this Policy to their supervisor or an appropriate senior employee.

### **Accessing Personal Mail**

Email may be used for incidental personal purposes. This does not include uses requiring substantial expenditures of time, uses for profit or uses that would otherwise violate Group Policy with regard to employee time commitments or Company equipment. Access to personal email (such as Hotmail) using workplace computers should be restricted to lunch periods.

Any webpage or email, including online emails such as "Hotmail", is also subject to PRL's acceptable use guidelines contained in the Group Policy.

### **Email and Privacy**

PRL provides email to assist in conducting business; therefore emails are Company property and can be traced if necessary (even if messages have been deleted). The content of electronic communications is not the personal property of the employee. Like other forms of text-based communication, email is the property of the employer and will be treated as such.

## **Content of Mailboxes**

Mailbox contents must be kept to the minimum amount required for work purposes. Storage and backup of non-work related emails will not be allowed and the Company has the right to review mailbox contents which may be deemed non-work related.

## **Attachments**

To ensure optimal use of email capacity, attachments that are multimedia-based, programs or larger than 10MB are blocked by default. Contact the IT Manager when you have a business requirement to send or receive such attachments. Distribution of attachments to a large number of people should generally be avoided. It is recommended that attachments should be:

- Placed on the Internet and referenced by a hyperlink in the email;
- Scheduled to run after business hours; and
- Approved by IT Support before distribution.

The Internet connection is a shared resource. While routine email and file transfer activities do not affect service levels significantly, large file transfers and intensive multimedia activities will impact the service levels of other users. Users contemplating file transfers over 10MB per transfer, or interactive video activities, should schedule these activities after business hours, or early or late in the day.

## **Arrangements for Leave**

Staff taking leave must ensure that, in their absence, their mail-boxes are set up to:

- Provide automated replies to senders advising of their absence and providing email and telephone contact details of the person undertaking duties while they are away.
- Automated replies should be removed as soon as employees resume their duties.

## **Downloads and Viruses**

Employees are not to use email systems to download software unless it has been checked with appropriate virus software to ensure it is virus free.

## **Passwords**

The use of your computer, email and the Internet is monitored through an "user id" and access rights governed by a password personal to you. Do not divulge your password to others because you could be held responsible for their actions.

## Security

PRL has adequate security arrangements in place to protect the network from unauthorised access. Employees are required to support these security arrangements through the following actions:

- Access to the Internet should be through officially approved mechanisms only (normally through the firewall). The connection of stand-alone modems to individual personal computers must be authorised on a case-by-case basis.
- Where external access is to be provided, security controls will be established to ensure no alternative path to the Internet services can be gained from PRL applications. No exceptions or entry points will be allowed.
- When there is suspicion of a virus, staff must note the symptoms and any error messages appearing on the screen, isolate the workstation if possible, inform the IT Manager immediately and not attempt to transfer information to another computer.

## Logging Off

At the end of each workday, employees are to log off their workstations prior to departure. On Friday afternoons employees are to shut down their workstations.

## Monitoring

PRL may monitor, copy, access or disclose any information or files that are stored, processed or transmitted using Company equipment and services. The Company may monitor on a random or continuous basis to:

- Prevent de-standardisation of the computer network because of the downloading of unauthorised software.
- Ensure compliance with Company Policies.
- Investigate conduct that may be illegal or adversely affect the Company or its employees.
- Prevent inappropriate or excessive personal use of Company property.
- Be able to link Internet sites accessed with the user identification.
- Generate reports that link Internet sites with the user identification.

Employee email boxes will normally contain the emails they have sent and received. Network back-ups and archives may also contain copies of emails that have been deleted by the user. As well as the actual content of messages, the date and time the message was transmitted, received and opened, as well as the email address of the sender and recipients will normally be recorded. All email traffic on the PRL system is automatically logged and is subject to scrutiny by system administrators and auditors.

## **Breaches and Consequences**

Every employee has a responsibility to be ethical and efficient in their official or private use of Company property and services and to be productive in the use of their work time. Any identified use of equipment or services thought to be inconsistent with PRL Policies will be investigated. Inappropriate use may be subject to disciplinary action, including termination of employment and/or criminal prosecution.

## **Site Based Policy**

PRL acknowledges that different mining operations and locations may have different needs for Internet usage and, as such, may have different policies specific to those sites. This will be defined by the Operations Manager at site and this Policy will be given upon commencement of your employment. The provision of any additional site-based policies will not, however, negate the requirements and obligations of the Group Internet and Email Policy on the employee.

## **Consequences of Breach**

If any use of the Internet or email services is found to be contradictory to PRL Policies, the user may lose access privileges and be disciplined through the company's disciplinary procedures.

Violation of the Group Internet and Email Policy may result in a recommendation to revoke access to computing and communication facilities, result in disciplinary action and/or termination of employment, and where appropriate be referred to the WA Police Service.

Management will be informed of all breaches of this Policy. Offending employees will receive written notification of their breach and will be counselled on their actions including:

- Corrective action to be taken.
- Disciplinary action to be taken.
- Consequences for subsequent breaches.
- Termination of Employment

Inappropriate use of the Internet or email facilities may result in the following:

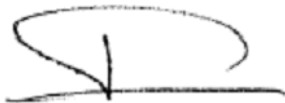
- Referral to civilian law enforcement authorities for criminal prosecution; or
- Other legal action including action to recover civil damages and penalties.

If you would like clarification of any of the matters in this Policy, do not hesitate to ask your Supervisor or IT Manager.

**Author**

IT Manager, Perth Office.

**Approved by:**

A handwritten signature in black ink, appearing to be 'Peter Harold', written over a horizontal line.

**Peter Harold**  
**Managing Director**

3 September 2008