THE RICE MARKETING BOARD FOR THE STATE OF NEW SOUTH WALES

RESPONSIBLE COMPUTING POLICY

Version	Author	Date Approved by Board
2009-1	Gillian Kirkup	24 March 2010
2017-1	Carol Chiswell	12 May 2017

Purpose

This policy is intended to define acceptable and unacceptable computing uses and practices within the Rice Marketing Board for the State of New South Wales (the Board) computing environment.

Scope

This policy covers all computing environments including desktop, laptop, network, remote access, email and Internet and all people using these environments including contractors, casual, full-time and part-time staff and Members.

The availability of networked information via the Board's network does not constitute endorsement of the content of that information by the Board. The Board's Secretary provides individuals access to the Board's systems where appropriate for authorised use only.

Responsibility

This policy is reviewed by the Board annually and is managed and implemented by the Board's Secretary.

Communication

In order that all employees are aware of this policy, the policy is made visible in the following ways:

- Current employees including Members - Revisions are notified when approved by the Board.
- New employees – All Policies are included in the induction program.
- Contractors, Consultants and other third parties – The Board's Secretary ensures that each contractor, consultant or other third party is aware of the policy.

Definitions

"**Account Owner**" - The person with responsibility for the named account.
"**User**" – Anyone authorised to use the Board's PC and Network Environment as set out in the "Scope" section of this document.
"Electronic Communications" – Communication using computer based tools that facilitate primarily non face to face communications. E.g. Email, Desktop Faxing

Policy

The Board encourages and condones the ethical and legal use of computing resources and will not provide legal defence for illegal or unethical use of its computers or software.

Following are the principles governing the use of the Board's computer hardware, software, electronic information systems and networks, including the Internet, email and the World Wide Web.

The Board's computer hardware, software, electronic information systems and networks, including the Internet, World Wide Web and email through the Board is for the use of authorised users in accordance with the Board's Responsible Computing Policy and may not be used to cause offence to others. Unauthorised usage of these facilities is prohibited.

Non-adherence to these requirements can result in disciplinary action and may include termination of employment.

In addition, individuals may be prosecuted to the full extent of the law.

General Use Guidelines

Users are specifically advised that they must have no expectation of privacy for any Internet or email based communications, whether business or personal, when using the Board's systems. All restrictions placed on these communications are in accordance with the *Workplace Surveillance Act 2005* and detailed clearly within this Policy. The current version of this document is available on request from the Secretary of the Board. it is the responsibility of each user to read and understand the updated content and contact the Board's Secretary if clarification is required.

The Board's Secretary will make every endeavour, via both automated and manual processes, to protect the integrity of the network, the information contained therein and the Board's reputation. Measures have been put in place to protect the security of the Board's Intellectual Property and corporate information, legal liability and to reduce exposure to, and damage from, other security threats such as computer viruses. For the indicated reasons, a secured copy of all emails will be retained in corporate archives.

An automated system is in place restricting access to websites that would be regarded by reasonable persons to be offensive, in contravention of the Responsible Computing Policy or that are deemed a security threat. Where inappropriate usage is reported, follow-up actions will occur and may include disciplinary action.

The Board uses automated systems to constantly monitor and filter all email sent from or received by the email system to prevent email;

- Considered to be an unsolicited commercial electronic message within the meaning of the *Spam Act 2003*.
- Considered to contain content or attachment that would be regarded by reasonable persons as being, in all the circumstances, menacing, harassing or offensive.

- Containing any content that would or might have resulted in interference with, or damage to the Board's systems (e.g. viruses or other malicious content).
- Containing any content that is otherwise covered in this policy or that may affect the reputation of the Board.

Users' outbound communications must not be inflammatory, harassing, defamatory, offensive, disruptive to other's operations, or otherwise reflect poorly on the reputation or image of the Board.

Users must understand that information passing through corporate links to the public Internet and beyond may be intercepted and/or monitored by other parties outside of the Board.

All users must use good judgment in utilising shared computer resources and avoid both printing and storage of unnecessary files and emails.

Use of the Board's computer systems for private financial gain is prohibited. E.g., using the Board's computers to run a word processing service is not permitted.

Security Guidelines

Users are individually responsible for understanding and respecting the security policies of the Board's computer systems. Users are individually accountable for their own behaviour. This applies not only to our corporate systems, but also to any other system accessed from our corporate systems.

Users have a responsibility to employ available security mechanisms and procedures for protecting corporate data. They also have a responsibility for assisting in the protection of the systems they use and alerting the Board's Secretary of any possible breaches of this security.

When leaving your PC for more than a minute, ensure it remains secure by "locking" it. When leaving the office for the day ensure that your computer is either "locked" or "logged off". The Board's computer policy includes the use of a screensaver being automatically invoked after a fixed period of inactivity (currently 10 minutes).

Laptop users are responsible for the security of their assigned device. The laptop must be either secured or taken with you when leaving for an extended time away from the office. If a laptop must be left in a vehicle, do not leave it visible within the cabin. Lock it in the boot. Do not leave laptops unattended in public places such as cafes or airports.

The Account Owner on the Board network is responsible for all activity performed under their account. Each person must use only their own account. It is prohibited to allow someone else to use your account. If someone else requires certain privileges or access to particular data their own account should be modified to allow them to do this, or an account should be requested if they do not have one.

The password to each account must be kept confidential. It must not be included in any documentation or included in any automatic logon on the Board's network nor disclosed to anyone including family, colleagues or friends. Password sharing is strictly forbidden.

Avoid using a password that could be easily guessed. A good password should consist of a combination of letters, numbers, spaces and special characters.

Software patches or updates obtained from officially supported vendors must adhere to vendor-recommended security procedures.

Software Guidelines

All software purchases and requests for additional licenses must be approved by the Board.

Users may not duplicate any licensed software or related documentation for use either on Board premises or elsewhere unless the Board is expressly authorised to do so by agreement with the licenser. Unauthorised duplication of software may subject users and/or the Board to both civil and criminal penalties under the Australian Copyright Laws. All software used (including screensavers) must be licensed.

All software purchases are to be approved prior to installation on Board owned equipment.

Hardware Guidelines

Computer software and hardware purchases cannot be connected to the Board's network unless they remain compliant with software licensing obligations and contain the appropriate level of software protection programs (see above). This includes but is not limited to PCs (all varieties), modems, and Mobile Computing devices such as Windows Mobile enabled devices, mobile phones or similar devices.

Remote Access Guidelines

When access is required to Board network resources from home, or when travelling, for business purposes, access is via a Virtual Personal Network (VPN) that has been approved by the Board and standard login requirements and terms and conditions of this policy will apply. Access will only be allowed on laptops or desktops provided by the Board.

Internet and Electronic Communications Use Guidelines

Where possible Email should not be used for large file transfers. If necessary, attachment size should be limited to no more than 35 megabytes.

Information integrity cannot be assumed for information obtained from the public Internet. Unless verified, this information should not be used for business critical application.

All Board related information services provided through Web servers or other means must have the corporate “look and feel” and be consistent with existing publications. This includes use of the corporate logos.

For external emails, a signature text including name, position and contact details, must be used at the bottom of email messages.

Acceptable Uses of the Internet and Electronic Communications

- Exchange of information for professional and work related purposes.
- Remaining professionally current.
- Debate of issues in a field of knowledge.
- Business related research and development.

Unacceptable Uses of the Internet and Electronic Communications

- Any purpose contrary to the corporate objectives of the Board.
- Electronic harassment of any kind.
- Use of language that would be regarded by reasonable persons as being unprofessional, menacing, harassing, offensive or that may impact on the reputation of the Board.
- Downloading, uploading, copying, distributing or viewing any form of pornographic, racist or discriminatory content; any content that pertains to any form of criminal activity; any content which may be considered by reasonable persons as offensive. This includes but is not limited to web sites, email and any form of removable media.
- Compromising the privacy of users or confidentiality of data.
- Wasting of resources (people, capacity, and computer). Remember that the cost of delivering and storing data is not only the amount of time connected, but also the infrastructure, network bandwidth, and people resources that make it possible. These are costs not only for the receiver of the data, but for the sender as well.
- Seeking to gain unauthorised access to resources on the Internet.
- Alteration or destruction of the integrity of computer-based information.
- Playing or loading computer games on Board equipment.
- Propagating chain letters, virus hoax emails, forwarding joke emails/ documents or images.

Email Etiquette Guidelines

Email as a medium of communication has become an indispensable tool for the Board’s business. There are no 'official' rules governing email based communication, however, as a general rule email etiquette involves basic courtesy, respect and ethics. Below are some guidelines that, if followed, should ensure that the recipient of your email will be more likely to read and act on it;

- Make the subject line a concise summary of the body of the email. This will ensure that the recipient will see at a glance the purpose of your message.

- Keep emails concise and to the point. Avoid lengthy renditions of the issue but ensure that you include enough contextual information so the recipient will understand the content.

- Avoid typing in capital letters or overdoing punctuation. (i.e. !!!!!) This is considered equivalent to shouting and quite rude.

- Avoid replying to emails when you are angry. This can lead to an angry outburst that you later regret. Wait until you have calmed down to write your reply.

- Ensure that you use language that is professional and polite. Avoid using language that would be regarded by a reasonable person to be offensive or explicit.

Further information

For further information concerning the Board’s Responsible Computing Policy, please contact:

The Secretary
The Rice Marketing Board for the State of New South Wales
PO Box 151
LEETON NSW 2705

Telephone: (02 6953 3200
Facsimile (02) 6953 7684

E-mail: secretary@rmbnsw.org.au