



## POLICY - COMMUNICATION & INFORMATION TECHNOLOGY

DATE OF ORIGINAL ENDORSEMENT:	13 February 2015
DATE OF EFFECT:	
DATE LAST AMENDED: Version control : V2/2017 – 31 <sup>st</sup> March	V3/2017 – 23rd November 2017
AUTHOR	Kym Ward – Manager Member Services & Dave Wiseman – IT Manager

### 1 Purpose

The Public Service Association (PSA) (CPSU) recognizes the importance of providing clear and transparent employment policies to all our staff. The PSA is committed to ensuring that its decision making and processes are above reproach.

This policy is designed to ensure the Communication and Information Technology of the PSA is a productive tool and is kept safe and secure.

This policy should be read in conjunction with Social Media Policy (TBA)

## **1 SOURCES OF AUTHORITY**

- 1.1 As per Rule 54(i) and in line with Chapter B of PSA By-Laws it shall be the responsibility of the General Secretary to implement this policy and to monitor its performance.
- 1.2 Workplace Surveillance Act 2005 (NSW).

## **2 APPLICABILITY**

- 2.1 This policy applies to PSA staff (including casual, temporary or seconded), as well as contractors and consultants engaged by the PSA.
- 2.2 This policy also applies to officials of the PSA provided with information communication and technology ("ICT equipment") or access to ICT resources.
- 2.3 This policy applies to all use of Internet and email services where such use is undertaken through the PSA's network, regardless of the location from which it is accessed.

## **3 RESPONSIBILITIES OF STAFF**

- 3.1 All staff are personally accountable in their use of work resources and are responsible for ensuring that:
  - Official resources are used ethically and lawfully.
  - Due economy and efficiency is applied in the use of official resources.
  - Appropriate steps are taken to protect confidentiality and privacy.
  - The requirements of this policy and any associated guidelines or procedures are adhered to.
  - Suspected breaches of this policy are reported to a Supervisor or Manager in the first instance.
- 3.2 Sufficient care must be taken of ICT resources when issued to staff. If damage or complete loss (including repeated losses) of an item occurs as a result of negligence, willful or malicious damage the individual may be held liable for replacement or repair costs incurred.

## 4 USE OF INTERNET AND EMAIL

- 4.1 Staff are required to read and agree to the **Acceptable Use Acknowledgement and Notification** displayed upon each occasion of logging in to a PSA computer.
- 4.2 In agreeing to this notification, staff confirm that they are authorised to use the PSA's information systems, services and facilities and that they will only use the information systems, services and facilities that they are authorised to use.
- 4.3 Staff also agree to the following conditions of use in respect to this notification:
- Access to the PSA's information systems, services and facilities is restricted to authorised individuals.
  - Information on the PSA system is confidential and must not be disclosed to unauthorised persons, or accessed for personal reasons.
  - Authorised users are not permitted to disclose their user identity or password to any other person unless there is a reasonable excuse or to allow their access identity to be misused.
  - Authorised users may be subject to disciplinary proceedings where the authorised user discloses their user identity or password to any other person without a reasonable excuse.
  - Utilising ICT resources to seek out, access or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature or which prejudices the work of the PSA, is prohibited and may result in disciplinary action.
  - The use of ICT equipment and ICT resources is subject to ongoing and continuous surveillance to validate that use is in accordance with this policy.
  - That this policy and the **Acceptable Use Acknowledgement and Notification** constitute notice of surveillance as required by Section 10 of the Workplace Surveillance Act 2005 (NSW). As such, surveillance will commence 14 days after this notification is first posted and will be carried out both automatically and by means of regular manual monitoring of information or files stored, processed or transmitted using the PSA's equipment and services.
- 4.4 The use of the Internet or email to make or send fraudulent, unlawful, offensive or abusive information or messages is prohibited. All staff are to report any such messages to a Manager in the first instance.
- 4.5 Any staff member found to have made or sent such information or messages may be subjected to disciplinary action and/or criminal prosecution.

- 4.6 Unlawful and inappropriate use of the Internet and email includes, but is not limited to, creating, sending, communicating or accessing information that may:
- Damage the reputation of the PSA or its officials or staff;
  - Be knowingly misleading or deceptive;
  - Result in victimisation or harassment;
  - Lead to criminal penalty;
  - Expose the PSA to civil liability;
  - Willfully facilitate unauthorised access, modification or impairment of data on a computer;
  - Be reasonably found to be offensive, obscene, threatening, abusive or defamatory;
  - Include pornographic or sexually explicit material in the form of images, text or other offensive material;
  - Discriminate against, harass or vilify colleagues or any member of the public on the grounds of sex, pregnancy, age, race (including colour), nationality, descent or ethnic background, religious background, marital status, disability, HIV/AIDS and homosexuality or transgender.
- 4.7 Staff must not encourage or assist others to engage in unlawful or inappropriate use of the Internet and email.
- 4.8 Staff are permitted to access the PSA and CPSU NSW or other legitimate PSA Facebook/twitter accounts in work time, using desktop computers or their supplied work mobile. Comments posted on these sites are not as a PSA representative or to be attributable to the PSA, unless you have consent from the General Secretary. (i.e. some employees are responsible for posting and commenting on behalf of PSA as per their job description).

## **5 RESTRICTED ACTIVITIES**

5.1 The PSA reserves the right to audit and remove any illegal material from its computers without notice

5.2 Staff must not:

- Intentionally access, create, transmit, distribute, or store any offensive information, data or material that is prohibited by federal or NSW laws or regulations. The PSA reserves the right to audit and remove any illegal material from its computers without notice.
- Use Internet or email services for personal business purposes or for personal financial gain.
- Unless clearly authorised by Central Council or the Executive, use, transmit or incorporate in communications any form of advertising or sponsorship.
- Represent themselves as another person when sending email or posting information to the Internet, whether that person is real or fictional.
- Use another staff member's account to send email messages or to access the Internet unless given express permission to do so.
- Send emails in another person's name, without their express consent.

- Undertake any form of computer hacking (i.e. illegally accessing other computers).
- Subscribe to social networking sites using their PSA email address where their PSA email address is readily accessible to other users, unless expressly approved in advance by the General Secretary.
- Subscribe to social networking sites using their PSA mobile phone number with the exception of 4.9.
- Use the Internet or email for unauthorised activities such as gambling, gaming, accessing chat lines, transmitting inappropriate jokes, pornography or sending junk programs. ( Footy tipping competitions, Melbourne Cup Sweeps etc., are permitted with the General Secretary's prior approval )
- Use Internet services for internet relay chat and FaceTime chat at any time without approval.
- Automatically forward email messages to an external email account without approval from the General Secretary.
- Automatically forward email messages from personal email accounts to their PSA email account that is not work related.
- Transmit material in breach of copyright or material over which intellectual property rights exist without the express permission of the owner.
- Externally transmit an advertisement of goods or services available for sale or hire. Undertake any activity intending to have a detrimental effect on storage, processing or communications network services (i.e. viruses, malware, chain letters etc.)

## **6 BROADCAST OR 'ALL STAFF' MESSAGES**

- 6.1 Access to the 'All Staff' distribution list is restricted.
- 6.2 Authorisation to send a message to this distribution list must be obtained from the General Secretary.
- 6.3 The General Secretary will then delegate the task of sending the email on behalf of the staff member who made the request.

## **7 PERSONAL USE**

- 7.1 Personal use of the Internet and email is a privilege and should be treated as such.
- 7.2 The PSA recognises that reasonable personal use of the Internet and email are one of the ways that a work life balance can be achieved. For this reason you may use the PSA's network for reasonable personal use such as research, learning or Internet banking
- 7.3 Internet or email use for personal purposes is subject to the same terms and conditions as otherwise described in this policy.
- 7.4 Due to the impact upon the network you should not download programs, games and sound files without Management approval.

- 7.5 Staff members reasonably suspected of abusing personal use of the Internet and/or email may be asked to explain such use or have the contents of their messages accessed.
- 7.6 Unreasonable or inappropriate personal use of email or the Internet may be the subject of disciplinary action.
- 7.7 All ICT resources issued to staff remains the property of the PSA. Upon ending engagement or employment of the association, the association is not obligated to release resources to the individual under any circumstance, unless authorised by General Secretary.
- 7.8 For personal security reasons, staff should not use their PSA mobile phone number or email address for internet banking verification.
- 7.9 Staff should not enter in to any subscription services whereby billing is charged against the PSA mobile phone contract unless prior authorisation is given by the General Secretary.
- 7.10 ICT equipment is not to be used for any Secondary or Private employment.

## **8 EMAIL BACK-UP**

- 8.1 The PSA regularly backs up the email service to protect the reliability and integrity of the system.
- 8.2 As this backup process results in the copying of email messages to a secondary storage device in accordance with standard backup procedures, email messages that have been deleted by staff members may still be accessible via the backup storage device.
- 8.3 The PSA reserves the right to archive email for governance purposes in a transparent manner in accordance to governance requirements.

## **9 SECURITY AND PRIVACY**

- 9.1 Authorised users are provided with a unique user ID to access the PSA network.
- 9.2 Activity against each unique user ID is continually logged and monitored.
- 9.3 Staff are responsible for all Internet activity and email use logged against their user ID.

## **10 MONITORING**

- 10.1 The PSA has the right to monitor, copy, access or disclose information or files that are stored, processed or transmitted using the PSA's equipment and services.
- 10.2 The PSA has the right to use geo-location services embedded within devices to locate the device if deemed necessary.
- 10.3 The PSA monitors the use of Internet and email services in accordance with the Workplace Surveillance Act 2005.
- 10.4 Email and Internet services are automatically monitored by software applications to ensure that viruses, spam and other inappropriate messages do not enter the PSA's network.
- 10.5 The PSA reserves the right to limit the size and volume of emails sent and received on the PSA system, as well as the amount of emails retained by the PSA.
- 10.6 The PSA will ensure that Internet and email usage is adequately monitored to:
  - Ensure compliance with this policy.
  - Investigate conduct that may be inappropriate, illegal or contrary to this policy.
  - Prevent inappropriate or excessive personal use of the PSA's property and services.
- 10.7 Monitored information may be viewed or disclosed to the Executive, Central Council or others where required by law

## **11. INFORMATION AUTHENTICITY AND QUALITY**

Do not base any critical decisions on information accessed through the internet technology, including email without first confirming the authenticity and quality of that information.

## **12. BROAD DISCLAIMER**

The following disclaimer has been approved and should be used at the foot of all emails:


*"This email and any attachments may contain privileged and confidential information and is only for the named recipients. If received in error, please delete the email and tell us by return email. If you are not the named or authorised recipient you must not copy, distribute or take any action in reliance to it. The PSA cannot guarantee that what you receive is what we send. If you have any doubts about the authenticity of an email purportedly sent by the PSA please contact us on 1300 772 679 immediately."*

### 13 GLOSSARY

Email	A message, including any attachments, sent in an electronic format from one user to one or more other users via a computer network.
ICT equipment	The equipment covered under this policy supplied and/or maintained by the ICT Section of the PSA, including:  Computers <ul style="list-style-type: none"> <li>• Monitors</li> <li>• Laptops</li> <li>• Projectors</li> <li>• Mobile Phones and associated mobile numbers</li> <li>• Desk Telephones</li> <li>• Film video and photographic equipment</li> </ul> Photocopiers and Facsimile machines
ICT resources	These resources include, but are not limited to, the network of the PSA, computer systems, ICT equipment, hardware and software, Internet access, electronic mail, telephony and data.
Official of the PSA	Any honorary official or paid official who holds office within the PSA. This includes the Executive and delegates of the Central Council.
Personal business purposes	Secondary employment or home business related purposes. Work related to employment in another workplace or environment.
Telephony	Communications made using a desk or mobile phone, facsimile, SMS or MMS.
Unauthorised person	Any individual who is not seconded or directly employed by the PSA or who has not been elected to hold office within the PSA.

### 14. Breaches of this policy

Any sustained breaches of this policy may lead to disciplinary action, pursuant to the PSA Performance & Conduct Policy.

	DATE & SIGNATURE
ENDORSED BY GENERAL SECRETARY:	
CENTRAL COUNCIL ENDORSEMENT/ RESOLUTION NUMBER (if applicable)	