Internet, Email and Systems Use Policy

1. PURPOSE

1.1 This policy outlines the acceptable use of technology hardware, systems and services at Paddle Australia (PA) and its State Paddle Associations (SPAs) (each referred to singularly as "**the Organisation**") and associated protocols.

2. APPLICATION

2.1 This policy applies to all Users wishing to access the Organisation's Information Systems.

2.2 Effective security requires the participation and support of all the Users who deal with the Organisation's Information Systems. It is the responsibility of every User to know these guidelines and to conduct their activities accordingly.

2.3 Inappropriate use of the Organisation's Information Systems exposes the Organisation to risks including, but not limited to, virus attacks, compromised network systems and services and legal claims.

3. DEFINITIONS

3.1 "**Executive**" is a senior management representative of the Organisation, which includes the CEO and other Executive Officers

3.2 "**Information Systems**" include the Organisation's owned, leased or licensed internet / intranet / extranet-related systems, including, but not limited, to computer equipment, mobile phones, peripherals, software, operating systems, storage media, network accounts providing electronic mail and internet browsing.

3.3 "**Users**" includes Workers, contractors, consultants, third party staff and others who are authorised to use the Organisation's IT / Digital network and systems.

3.4 "**Workers**" includes employees, independent contractors or representatives of independent contractors, work experience students and other volunteers.

4. MAIN BODY OF POLICY/GUIDELINES

4.1 General Use and Ownership

a) Users should be aware that the data they create on the Organisation's Information Systems remains the property of the Organisation. In consideration of the need to protect the Organisation's electronic assets, the Organisation cannot guarantee the confidentiality of information stored on any of the Organisation's Information Systems, including devices.

b) Users are responsible for exercising sound judgment regarding the reasonableness of personal use of the Organisation's Information Systems. When in doubt Users should consult their manager.

c) For security and network maintenance purposes, Users may from time to time have their use of the Organisation's Information Systems monitored by the Organisation.

d) The Organisation reserves the right to audit networks and systems which form part of the Organisation's Information Systems on a periodic basis to ensure compliance with this policy.

e) Users are responsible for the maintenance and upkeep of operating system and anti-virus/malware solutions installed on equipment or devices issued to them for the purpose of limiting exposure to internet based threats

4.2 Security and Information Storage

a) Users must not open e-mail attachments received from unknown senders, which may contain viruses, malicious e-mail payloads or any other form of malicious code.

b) Users are to notify their manager and the ICT Helpdesk if they unintentionally open e-mail attachments received from unknown senders, which may contain viruses, malicious e-mail payloads or any other form of malicious code.

c) The Organisation takes no responsibility for any personal data stored on equipment provided as part of the Organisation's Information Systems.

4.3 Unacceptable Use

a) Under no circumstances is a User authorised to engage in any activity that:

i. is illegal under local, state, federal or international law;

ii. involves the creation or distribution of any disruptive or offensive messages;

iii. involves comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin. In addition, sending or receiving any material that is obscene, hateful or objectionable material;

iv. involves pornographic or other sexually explicit or offensive material;

v. involves uploading, downloading or transmitting commercial software or copyrighted material in violation of its copyright. This includes, but is not limited to .mp3 or .mp4 files;

vi. involves undertaking personal commercial ventures or business activities not related to the Organisation's business.

b) The matters referred to in sub-clause 4.3a above are by no means exhaustive.

4.4 System and Network Activities

The following activities are strictly prohibited:

i. introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan Horses, e-mail bombs, etc.);

ii. revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home;

iii. using the Organisation's Information System to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;

iv. providing information about, or lists of Workers, athletes, members, contractors or suppliers to parties outside the Organisation without prior approval from the relevant Executive;

v. accessing, viewing, posting, downloading, storing, transmitting, sharing, printing, distributing or soliciting of any information or material that the

Organisation views as racist, pornographic, obscene, abusive or otherwise offensive.

4.5 Email and Communications Activities

a) Personal email usage during work hours is to be kept to a minimum.

b) Users should ensure their personal businesses' websites and/or details are not included in email signatures or promoted in official Organisation correspondence without the written permission of the relevant Executive.

c) Users should ensure that when they will not be able to access their emails for more than 24hours a suitable "Out of Office" message is set-up. The message should advise an appropriate alternate email contact for urgent matters and should be removed immediately upon return.

d) The following activities are strictly prohibited:

i. sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);

ii. sexual comments or images;

iii. solicitation of non-business causes (including but not limited to political, religious causes unless the activity is the Organisation's sponsored or sanctioned activity);

iv. chain-letters;

v. gender-specific comments, or any comments that might offend someone on account of his or her age, gender, sexual orientation, religious or political beliefs, national origin or disability; and

vi. messages which have the potential to be viewed as defamatory, threatening or obscene.

5. RESTRICTING OR BLOCKING ACCESS

5.1 The Organisation may, at any time and without notifying Users, restrict or block access to various internet sites and applications.

5.2 Any use of programs by Users to in any way subvert the Organisation's filters in order to access blocked internet sites and/or applications will amount to a breach of this policy.

6. PASSWORD PROTOCOL

6.1 All system-level passwords (e.g. application administration or accounts administration) must be changed when a User who had the password leaves the Organisation, or at a minimum, on a quarterly basis.

6.2 All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed every two months.

6.3 Passwords must not be inserted into email messages or other forms of electronic communication or placed on printed or handwritten notes.

6.4 All Users are required to set a strong password which is defined as having the following chacteristics:

a) Both upper and lower case characters (e.g. a-z, A-Z)

b) Have a digit and/or punctuation character as well as letters (e.g. 0-9,.$%^&*!#()?

c) Not based on personal information e.g. name, family or pet's names.

6.5 Passwords are to be treated as sensitive confidential information. Users are not permitted to share the Organisation's passwords with anyone, including but not limited to other Users, family or friends.

7. PA AND SPA WEBSITES

7.1 The only official websites of the Organisation are:

paddle.org.au

nsw.paddle.org.au

qld. paddle.org.au

sa. paddle.org.au

tas. paddle.org.au

vic. paddle.org.au

paddlewa.asn.au

education.paddle.org.au

paeducation.paddle.org.au

paddleprep.paddle.org.au

paddleoz.paddle.org.au

helpdesk.paddle.org.au

paddlepower.paddle.org.au

paddlehub.paddle.org.au

whitewater.paddle.org.au

oceanracing.paddle.org.au

polo.paddle.org.au

marathon.paddle.org.au

wildwater.paddle.org.au

slalomage.paddle.org.au

slalom.paddle.org.au

sprint.paddle.org.au

marathonwa.paddle.org.au

wildwaterwa.paddle.org.au

sprintwa.paddle.org.au

slalomwa.paddle.org.au

paddleabouttasmania.paddle.org.au

paddlesmartvictoria.paddle.org.au

Approval must be obtained in writing from the relevant Executive to establish other websites for specific events and projects.

7.2 Users must not advertise any other site as being a source of official information from the Organisation.

8. BREACH OF THIS POLICY

8.1 All Users are required to comply with this policy as amended from time to time.

8.2 Any breach of this policy may result disciplinary action, up to and including termination of employment or engagement with the Organisation.

8.3 Any third-party agreement where a third party requires access to the Organisation's network must include this policy. Any third-party supplier not complying with this policy could have actions taken against them including, but not limited to, termination of contract.