IT Resources Acceptable Use Policy
For External Parties

Introduction: This policy aims to ensure visitors to AISWA and external users of AISWAs IT resources and equipment are provided with a framework to identify the standard of acceptable use in relation to computing equipment and/or resources as expected by the Association.

Scope and Application: This policy applies to all visitors of AISWA and external users who may need to use AISWA computing equipment and/or resources. This policy will be reviewed and amended as required *(see footer for policy review date)*.

Please read this policy carefully, and then indicate your acceptance of the policy by agreeing to the Terms and Conditions which form part of the online registration process.

AISWA appreciates that at times external parties or visitors to the organisation (teachers attending workshops, presenters etc) do use AISWA equipment and at times must access the internet through AISWA's connections.

This statement sets out the Acceptable Use Policy of AISWA and it applies to all visitors who use AISWA equipment or access the internet via AISWA.

AISWA views breaches of this policy extremely seriously. AISWA visitors need to be aware that where they undertake an action that is stated as prohibited in this policy, they become liable to incur restrictions on future access.

1. Ownership
Internet and e-mail systems (including but not limited to computer equipment, software, operating systems, email, public folders, Intranet data) are the property of AISWA.

2. Privacy of Communications
Communications on these systems are not private. While a reasonable level of privacy is available, users should be aware that the data they create on the corporate system remains the property of AISWA and usually can be recovered even though deleted by the user. Despite security precautions, it may be possible for an unauthorised user to access stored files.

3. Monitoring
The organisation reserves the right to monitor all usage by External parties and to recover the contents of any communication in the interests of ensuring proper working order, appropriate use by visitors and the security of data. The foregoing includes accessing user files for any purpose related to maintaining the integrity of the network or the rights of the organisation or other users or for any other reasonable purpose.

4. Personal Use
External parties should not use AISWA's system for any personal purposes.

External parties may not install additional software packages on any of the organisations computer systems over and above those provided by AISWA without the consent of the Information Technology Network and Office Systems Administrator.

5. Security and Organisational information
Information on the organisation's system is confidential, particularly information relating to the business affairs of the organisation or its members and is not to be disclosed unless it is authorised by the Executive Director.

External parties accessing AISWA equipment must use the resources only to undertake their presentation or workshop, and not undertake any other activities.

6. System integrity and copyright
All users should be aware that any information, software, or graphics on the Internet may be protected by Copyright Law regardless of whether a copyright notice appears. Licensing agreements may control redistribution of information from the Internet. External parties must never open, execute, or run unsolicited binary code e mail attachments due to the high risk of computer virus infection.

7. Restrictions and Prohibitions on Use and Access
Communications and Internet access should be conducted in a responsible and professional manner reflecting the organisation's commitment to honest, ethical and non discriminatory practice.

7.1 Data Security
External parties must only use the logon ID and password as provided by the Information Technology Network and Office Systems Administrator. They are responsible for all activity on their logon ID and must report any known or suspected compromise of their ID to the Information Technology Network and Office Systems Administrator. Unauthorised attempts to circumvent data security schemes, identify or exploit security vulnerability's, or decrypt secure data are prohibited.

Knowingly or recklessly running or installing (or causing another to run or install) a program (such as a "worm" or "virus") intended to damage or place an excessive load on a computer system or network is viewed as a very serious offence and is prohibited.

Forging the source of electronic communications, altering system data used to identify the source of messages or otherwise obscuring the origination of communications is prohibited.

7.2 Use of Equipment
Any use that violates Commonwealth, State law or regulation is expressly prohibited. Knowing or recklessly interfering with the normal operation of computers, peripherals, or networks is prohibited.

Using the organisation's equipment to gain unauthorised access to any computer system is prohibited.

Connecting equipment to the network that has not been provided or authorised by Information Technology Network and Office Systems Administrator is expressly prohibited. This restriction applies to, but is not limited to, laptop computers, PDA's, printers, hubs/switches, external disk drives, and wireless access points.

Approval to use USB drives or USB keys or similar portable memory devices is not needed from the Information Technology Network and Office Systems Administrator but external parties should obtain permission from the AISWA Consultant they are working with. USBs

should only be used where they come from a reliable source and where the data on them is not offensive or prohibited.

When external parties visit AISWA's premises, the staff member responsible for the external party must ensure that any equipment (other than USB) brought in is not connected to the organisation's network unless under the direction of the Information Technology Network and Office Systems Administrator.

7.3 Netiquette and Protocols
The use of AISWA's equipment to access, transmit, store, display, or request obscene, pornographic, erotic, racist, sexist or other offensive material (including messages, images, video, or sound) is prohibited.

Any use that is deemed to adversely affect or otherwise bring into disrepute the organisation is prohibited.

8. Amendment
This policy may be amended from time to time and users will be notified.

9. Disclaimer
AISWA will not be responsible for the misuse of computer networks or departmental Internet access or electronic mail by any external parties.

Should you have any questions regarding any of the above, please contact AISWA's Information Technology Network and Office Systems Administrator on (08) 9441 1600.