AISWA

Association of Independent Schools of Western Australia

IT Resources Acceptable Use
General - for External Parties

Introduction: This policy aims to ensure visitors to AISWA and external users of AISWA's 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 annually and amended as required.

NOTE: When reading this policy in relation to AISWA Professional Learning Events of any type – that is, 'in person', via 'webinar' or 'on-demand' - please read this in conjunction with the specific website and internet related Terms and Conditions published with those events. These are available online (via a link prior to accepting the Terms and Conditions of attendance) and as downloadable PDF documents found on the PL Events web page menu.

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. This also applies to a Bring Your Own Device (BYOD) used by a non-employee for AISWA work purposes. 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 non-employees and to recover the contents of any communication (inclusive of BYODs, portable storage devices, and cloud storage) in the interests of ensuring proper working order, appropriate use by non-employees 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

Non-employees may not use AISWA's system for any personal purposes.

Non-employees 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.

Non-employees are required to take all necessary steps to prevent unauthorised access to this information by diligent and careful use of the systems and equipment and by reporting suspicious activities. Failure to do so may result in a breach of the Privacy Act 1988 and non-employees may be held personally accountable for their actions.

Non-employees 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. Non-employees 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

Non-employees 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

a) Any use that violates Commonwealth, State law or regulation is expressly prohibited.

b) Knowing or recklessly interfering with the normal operation of computers, peripherals, or networks is prohibited.

c) Using the organisation's equipment or a BYOD, portable storage device, and cloud storage whilst on AISWA business to gain unauthorised access to any computer system is prohibited.

d) Connecting a BYOD, portable storage equipment (and cloud storage) to the network that has not been provided or authorised by the Information Technology Network and Systems Administrator is expressly forbidden.

These restrictions apply to, but are not limited to, laptop computers, PDA's, printers, hubs/switches, external disk drives, portable storage devices and wireless access points.

When non-employees visit AISWA's premises, the staff member responsible for the non-employee must ensure that any equipment 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, Emails, and Social Network Protocols and Legal Requirements

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

It is prohibited to send or forward e-mails containing libellous, defamatory, offensive, racist or obscene remarks.

It is also prohibited to use libellous, defamatory, offensive, racist, or obscene remarks on any networking site regarding AISWA or any employee or affiliate of AISWA. If a person using the AISWA IT Network becomes aware of such content on any social networking site of this nature, he/she must notify AISWA immediately.

Any person who uses the AISWA IT Network may not send or post messages to individuals or groups which:

- discuss or comment on the physical appearance of AISWA employees or employees of member schools, whether they are a recipient of the message or not;
- include comments of a sexual, racist or sexist nature or make inferences or comments about a person's sexual preferences;
- use abusive or offensive language;
- make inferences or comments regarding any physical disabilities of any employee of AISWA or a Member School.
- make inferences or comments that are libellous, defamatory, offensive, racist, or obscene about AISWA or any AISWA member school or bring AISWA or its affiliates into disrepute on any public or private networking site or blog.

The intention of the person in writing, posting or sending a message is irrelevant. If the message offends, humiliates or intimidates another person it may breach this policy and relevant legislation. AISWA will hold individuals liable for the content of offensive messages including those lodged on private web pages such as 'Facebook'. Note also that if a person uses AISWA's IT Network to use social networking sites for work purposes must set privacy settings to ensure that their personal information and private information about AISWA is not available for public access.

7.4 Hacking

‘Hacking’ is a criminal offence. Any person using the Internet access provided by AISWA for these purposes may be subject to prosecution as the proper authorities shall be notified of all such activities.

8. Disclaimer

AISWA will not be responsible for the misuse of computer networks or departmental Internet access or electronic mail by any non-employees.

Should you have any questions regarding any of the above, please contact the AISWA Information Technology Network and Office Systems Administrator.