WAIS Information and Communications Technology Users Policy

Owner: Finance and Operations Manager

Version: 2.1

Approved by: Executive Director

Effective from: 1 May 2011

Next review date: October 2018

Last Date of Edit: October 2016

WESTERN AUSTRALIAN INSTITUTE *of* SPORT

CONTENTS

1. Purpose

To guide WAIS staff to effectively and appropriately use Corporate Information and Communications Technology (ICT) assets, including the internet.

Staff are encouraged to make use of the ICT tools available to them, including mobile devices and the internet to their fullest potential to further the goals of WAIS. These tools should be used in a responsible, productive and informed way, conforming to security standards, network etiquette, customs and courtesies.

2. Scope

WAIS provides ICT resources to enable its users to do business in an ethical, effective, efficient and careful manner.

This policy outlines the acceptable use of the ICT systems, including the internet at WAIS and defines expectations and limitations when using WAIS ICT equipment. This policy is set so as to protect both WAIS and its employees.

WAIS ICT users are permitted and encouraged to use the internet where such use is suitable for business purposes and supports the goals and objectives of WAIS and its departments.

Corporate ICT assets include corporate information systems, software, data, and computing assets, which include but are not limited to computers, computer networks, printers, tablets, telephones and other related units of equipment.

3. Standards

3.1 WAIS ICT users will be notified of amendments to this Policy; however it remains the responsibility of the individual user to ensure familiarity with the contents of this Policy, and future amendments.

3.2 WAIS ICT users must not use ICT resources to search for, access, download or communicate any improper material.

3.3 The internet is to be used in a manner that is consistent with WAIS's standards of business conduct and as part of the normal execution of an employee's job responsibilities.

3.4 All data stored on any of the WAIS servers, computers and ICT equipment owned by WAIS is considered to be the sole property of WAIS.

3.5 Sensitive information produced by users that is created as part of their duties is not to be released to external bodies without approval from Departmental Managers or the Executive Director.

3.6 Users may not intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

3.7 Each user that is required to use any of the WAIS ICT systems will be issued with a logon ID and password and no user is to divulge their password to other users or persons at WAIS or outside of WAIS.

3.8 PCs must be logged off at the end of the day or when last used for the day, to prevent unauthorised use after hours.

3.9 Users should log out or lock the workstation when stepping away from the workstation for an extended period of time. WAIS will utilise a lock screen facility and workstations left idle more than ten minutes will be automatically locked.

3.10 No hardware items, such as PCs, printers, monitors, etc. may be removed from the WAIS office without written permission from the relevant manager.

3.11 No hardware or software (including portable equipment) will be loaned to users other than members of WAIS, unless prior approval in writing from the Department Manager.

3.12 WAIS will provide training for the use of specialised applications (DMS, Navision, Performax, etc.). WAIS will also provide training in general security awareness so that new WAIS employees will gain a better understanding of the ICT function and its permitted uses.

4. Principles of Conduct for usage of specific applications and information

The applications available via internet and their uses mentioned in this section are not to be considered exhaustive, thus users are to be familiar with the 'WAIS Internet Policy and Procedures'.

4.1 Internet:

4.1.1 The internet is a valuable business tool. WAIS staff are encouraged to use the internet to its fullest potential to further the goals of the Institute. Staff are under an obligation to use their access to the Internet in a responsible, productive and informed way, conforming to network etiquette, customs and courtesies.

4.1.2 Users may access the internet for personal purposes during normal work hours, however personal usage of internet should be moderated and not interfere with an employee's ability to carry out their daily work related duties.

4.1.3 Users may not visit internet sites that contain obscene, hateful or other objectionable or illegal materials.

4.1.4 Users may not make or post indecent remarks, proposals, or materials on the internet.

4.1.5 Information published to publically accessible web pages should be treated with equivalent care to that of other methods of distributing data. The information should be accurate and consistant with WAIS and Government policy. WAIS and its staff have a duty of care to ensure information available to the public on the web will not cause harm.

4.1.6 WAIS information should not be published on web pages that are not under the control of the Institute. Other organisations should be encouraged to create links from their sites to the WAIS website, should they wish to disseminate WAIS information.

4.1.7 All information to be published should be discussed with Management and the Corporate Communications Coordinator.

4.2 Electronic mail (email):

4.2.1 Electronic mail (email) is an electronic message sent by, or to a person, in correspondence with another person having email access.

4.2.2 Messages sent and received are retained on both the sending and receiving email servers until such time as the sender *and* recipient choose to delete the message, even after deletion, it may still be possible to retrieve a message from back up, therefore WAIS staff should treat email with the same consideration as physical mail.

4.2.3 It should be assumed that email is not secure and that any message sent may be read by people other than the intended recipient.

4.2.4 Users may send and receive personal emails, it is recommended that users maintain a separate personal email account for private usage. Personal usage of email should be moderated and not interfere with an employee's ability to carry out their daily work related duties.

4.2.5 Users may not send or receive material of a racist, sexist, obscene, or defamatory nature or which is intended to annoy, harass or intimidate another person.

4.2.6 Users may not use their WAIS email account to represent personal opinions as those of WAIS.

4.3 Social Media (e.g. Facebook, Twitter, YouTube etc.)

4.3.1 The use of social networking applications and sites has been the biggest shift in internet usage in recent times and therefore has significant impact on usage of the WAIS network.

4.3.2 Social networking can provide benefits to a number of different areas of the Institute, including communication with athletes and promoting the achievements of WAIS.

4.3.3 However communication via social networking applications and sites should not be regarded to be private communication, because:

4.3.3.1 Others can read posts to pages;

4.3.3.2 Others can view photos posted to pages; and

4.3.3.3 Others can post information or photos about you without your knowledge.

4.3.4 The following are guidelines to consider when interacting via social networking applications and sites:

4.3.4.1 Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the Institute. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the Institute;

4.3.4.2 Information published on your blog(s) should comply with WAIS's confidentiality and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums, and social networking sites;

4.3.4.3 Be respectful to WAIS, other employees, athletes, partners, and competitors; Social media activities should not interfere with work commitments;

4.3.4.4 Your online presence reflects WAIS. Be aware that your actions captured via images, posts, or comments can reflect that of the Institute; Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well; and

4.3.4.5 WAIS logos and trademarks may not be used without written consent.

4.4 File Sharing:

4.4.1 File sharing can be a productive method for the transfer of information between staff at WAIS and with colleagues and stakeholders outside of the institute, but should only be used to transfer authorised files, for the purpose of conducting business on behalf of the Institute.

4.4.2 Users should only use WAIS ICT resources to transfer files for the purposes of conducting WAIS business.

4.4.3 Users may not install or create files which contain elements of a racist, sexist, obscene, objectionable or defamatory nature or which are intended to annoy, harass or intimidate another person.

4.4.4 Users may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the organisation, or of the organisation itself.

4.4.5 Users may not examine, change, or use another person's files, output, or user name for which they do not have explicit authorisation.

4.4.6 Users may not install or upload any software of or suspect of being malicious by nature, illegal by copyright or not authorised by WAIS.

5. Security

5.1 All effort is taken to ensure that the WAIS network is secured against unauthorised intrusion, malware and other inappropriate access. Users also have a responsibility to ensure the security of the WAIS network

5.1.1 Users should use a password of sufficient complexity, in accordance with the WAIS ICT Policy.

5.1.2 Users should only visit trusted websites.

5.1.3 Users should not install software on their devices unless obtained from a trusted source. Any software to be installed on a WAIS owned laptop, computer or within the Citrix environment, may only be installed with the written permission of the Finance and Operations Manager.

5.2 Remote Access

5.2.1 Those users who have been granted permission to access WAIS ICT resources remotely are required to follow all relevant ICT guidelines set out in this policy and the ICT Management policy.

5.2.2 In addition remote users should take every effort to secure their own systems against viruses and other malware, and inappropriate access that may lead to the WAIS network being compromised. This includes but is not limited;

5.2.2.1 Install and update anti-virus and anti-malware software;

5.2.2.2 Make use of firewalls to prevent network intrusion;

5.2.2.3 Use sufficiently complex passwords to prevent unauthorised access.

6. Information

All information produced by users in an electronic format that is created as part of their duties and/or regular performance is considered to be the sole property of WAIS and shall not be shared with third parties without approval from Departmental Managers or the Executive Director. Information created in an electronic environment may be considered a record for the purposes of the WAIS Record Keeping Plan, ICT users should familiarise themselves with this plan, to fully understand their responsibilities.

Users are to consider the sensitivity of information that exists in electronic form, when sharing this information with other employees of WAIS. Users must not use information contrary to WAIS's code of conducts and privacy legislation, or any other WAIS policy.

WAIS via the ICT service providers, reserves the right to audit and remove any illegal material from its ICT resources without notice.

Users who have technology provided by WAIS that provides remote access to the WAIS operating system, are to ensure the resource is used only by those so authorised, and is kept safe and secure at all times.

7. Definitions

7.1 Improper material is material which could be considered by a reasonable person to be of an illegal, offensive, inappropriate, obscene, threatening, abusive or defamatory nature. Improper use of improper material comprises the distribution of private intimate content including written material and images.

7.2 Illegal activities are defined as activities in violation of State, Commonwealth, or International laws and internationally accepted etiquette.

7.3 Inappropriate use is defined as the violation of the intended use of the access to the WAIS network, internet, and/or purpose, goals and values of WAIS.

7.4 Obscene activities are defined as a violation of generally accepted social standards while using publicly owned and operated communication medium.