dacs
DEMENTIA & AGED CARE SERVICES

QUALITY PROCEDURE

DEMENTIA AND AGED CARE SERVICES
INFORMATION TECHNOLOGY SECURITY

1.0 OBJECTIVE

To establish and maintain procedures and guidelines that safeguards the integrity of the Alzheimer's Association of Queensland (AAQ) computer records and equipment and ensures that staff members are competent to operate AAQ computer equipment.

2.0 SCOPE

This procedure will cover all computer data records and equipment in use within the Association and will operate in conjunction with external regulations and legislation (e.g. Privacy Act) as appropriate.

3.0 RESPONSIBILITIES

3.1 The Chief Executive Officer (CEO) or nominated delegate will be responsible for:

(a) ensuring that the integrity of all computer data records is maintained;

(b) authorising access to personal or sensitive information in accordance with the Privacy Act 1988, where appropriate;

(c) authorising the installation of software programs in consultation with the AAQ's IT consultant

3.2 The Manager is responsible for ensuring that their staff are aware of this procedure and comply with its contents.

3.3 All staff are responsible for ensuring that the AAQ's IT systems are used responsibly and in accordance with this procedure.

4.0 PROCEDURE

Internet Access and Email Usage

4.1 Staff using the internet are responsible for ensuring that the internet is used in an effective, ethical and lawful manner in relation to their employment. Examples of acceptable use include but not limited to:

- Using web browsers to obtain information from reputable web sites pertinent to their position within AAQ;
- Accessing online computer networks and databases as required to perform work tasks e.g. iCare, RISKMAN, Moving on Audits (MOA) etc; and
- Using email for business purposes.

4.2 Staff must not use the internet for purposes that are illegal, unethical, harmful or non-productive. Examples of unacceptable internet use include but are not limited to:

- Conducting personal business such as banking, shopping, paying bills etc. or business on behalf of another employer during working hours';
- Transmitting any content that is, or could be perceived to be, offensive, derogatory, pornographic, fraudulent or illegal;
- Initiate or perpetuate chain email letters;
- Using applications such as instant messaging, Hotmail, P2P, Facebook etc.

4.3 Staff are not permitted to download software from internet sites without the express permission of the CEO or delegate. This does not include document files such as PDFs.

4.4 Staff should recognise that emails to outside parties represents the Association and therefore it is imperative that email correspondence is professional, well considered and grammatically correct. This also includes data that is recorded in programs such as iCare, RISKMAN, MOA. Computer entries must be clear, concise and unambiguous in meaning. Mischievous, malicious or vindictive content must be avoided.

Computer Viruses

4.5 Managers are responsible for ensuring that appropriate antivirus software is installed and maintained on all computers including laptops and servers.

4.6 Staff shall not knowingly introduce a software virus into AAQ computers.

4.7 Attachments, USB plugs and computer software from unknown sources shall not be opened on AAQ computers.

4.8 Any staff member who believes that their workstation has been infected by a virus shall immediately power off the computer and call AAO:s IT consultant.

Access Codes and Passwords

4.9 Access codes for Connx, RISKMAN, iCare will be assigned.

4.10 Staff members must formulate a password when access is established and must not disclose their password to others. Passwords must be changed immediately if it is suspected that they have become known to others.

4.11 Staff members are responsible for all computer transactions that are made using their ID and password.

4.12 Staff must ensure that they always log out of the password secure sites when leaving the workstation.

4.13 The Manager shall ensure that a staff member's access is removed as soon as the staff member leaves the employ of MQ or at the discretion of the Manager and or State Manager.

Physical Security

4.14 MQ computer hardware, software, data and networks must be protected from misuse, abuse, rough treatment, theft, unauthorised access, food, liquids, dust, extreme heat or cold.

4.15 Computer hardware should not be disconnected, modified or relocated without the express permission or knowledge of the AAO:s IT consultant, other than laptops.

4.16 The Manager will ensure that all staff maintain appropriate computer literacy skills of a level necessary to effectively complete work tasks and protect computer equipment and software from misuse.

Non-Compliance

4.17 Non-compliance with this procedure may result in disciplinary action being taken in accordance with MQ's procedures.

5.0 REFERENCED DOCUMENTS

Privacy Act 1988

AAQ-P-12	Privacy and Confidentiality
AAQ-P-16	Records Management
AAQ-P-30	Human Resources Disciplinary Action
AAQ-Form-01	Code of Conduct
	Staff Confidentiality Agreement

PPROVED BY: ________________________

CHIEFEXECUTIV OFFICER

DATE:04/09/2016