

ORKNEY ALCOHOL COUNSELLING & ADVISORY SERVICE IT POLICY

The aim of the policy is to provide guidance on the appropriate use of Orkney Alcohol Counselling and Advisory Service's computing and information assets.

It will also provide you with details of OACAS's Security Policy and your rights and responsibilities in relation to information security.

The intention of this Policy is to publicly demonstrate that we can be trusted to safeguard the confidentiality, integrity, and availability of the information we hold.

- *Confidentiality* – Data access is confined to those with specific authority to view the data
- *Integrity* – All system assets are operating correctly according to specifications and particularly in respect of accuracy, security and relevance.
- *Availability* – Data output is delivered to the point where it is needed, when it is needed.

Computer Use

Computer equipment should be used for OACAS purposes only; it may be used for self-development or other purposes at the discretion of your line manager.

Do

- ✓ Inform your line manager if you suspect any breach of security

Don't

- ✗ Use OACAS equipment for private commercial purposes
- ✗ Connect your personal computer to OACAS's network
- ✗ Attempt to gain unauthorised access to any system or modify information without authorisation
- ✗ Access or disclose information for any purpose not connected to work
- ✗ Install software without prior approval

Copyright, Designs and Patents Act 1988

You should only use software that has been licensed for use by Orkney Alcohol Counselling and Advisory Service. Installing or using unlicensed software could lead to the prosecution of OACAS and/or individual employees or volunteers. Periodic audits of equipment will be undertaken. Any unlicensed software or copyright protected files found will be removed; this includes games, MP3 and video files, text and image files.

Do

- ✓ Only use licensed software in accordance with the licence agreement
- ✓ Arrange for the removal of evaluation software once the evaluation period has expired
- ✓ Remember that information downloaded from the internet may be subject to copyright©

Don't

- ✗ Install software without permission. This includes free software
- ✗ Alter the set-up of your operating system
- ✗ Copy OACAS software for use on your home computer
- ✗ Install or use copyright material, e.g. maps or images on your machine unless you have permission

Data Protection

The Data Protection Act 1998 was passed to protect personal information held on computers or manual records. OACAS has to register details of all the types of personal information it collects with the Data Protection registrar. Data that is collected can only be used for the purposes for which it is registered and should only be disclosed to individuals and organisations defined in the registration. Breach of the Act could mean legal action being taken against OACAS and/or individual employees or volunteers.

Do

- ✓ Ensure that you are aware of OACAS's duties in regard to the Data Protection Act
- ✓ Check that OACAS's registration covers the information you hold and that data is accurate and up-to-date
- ✓ Notify the manager if a volunteer/employee or client makes a request to view details held about them. Check with the manager before disclosing information.

Don't

- ✗ Take personal information off site
- ✗ Disclose information to any unauthorised person
- ✗ Access systems to check personal information for yourself or a friend
- ✗ Keep personal information on the company laptop
- ✗ Leave personal information unattended on your desk, or on a home computer

Login Security

You are responsible for your own user ID and Password

Do

- ✓ Memorise your password
- ✓ Change your password regularly
- ✓ Report any suspicious attempts to access your system
- ✓ Log off from your computer when you leave the office

Don't

- ✗ Share your password with anyone else
- ✗ Use anyone else's user ID or password
- ✗ Write your password down and stick it on the monitor
- ✗ Choose passwords based on information about you that is easy to guess

Virus Protection and Backup

A virus is a programme that attempts to infect software. It may destroy or corrupt programs and data held on your computer. They can be spread through disks, e-mails or programmes found on the Internet.

- All OACAS's computers are regularly updated for their anti-virus and Windows software.

The data held on your machine can also be damaged or lost due to failure of the computer you are using.

- Backups on all computers are done on a regular basis with copies kept off the premises.

Do

- ✓ Ensure that all disks and e-mail attachments are virus checked before use
- ✓ Contact the System Administrator if you suspect your machine has been infected

Don't

- ✗ Install files or programmes unless authorised to do so
- ✗ Use your computer if you know or suspect it has a virus
- ✗ Not save critical or important data anywhere except in "My Documents" folder on your computer, or in a designated folder that the System Administrator is aware of.

Internet, Remote Access, and E-mail Access

OACAS provides access to e-mail facilities, the Internet and World Wide Web to support OACAS's business.

You should be aware that Internet access can be monitored and OACAS reserves the right to read e-mails sent and received by its employees and volunteers.

Do

- ✓ Use the Internet and e-mails to support OACAS business
- ✓ Report immediately any accidental access or receipt of inappropriate materials from the Internet or e-mail to the System Administrator
- ✓ Remember that E-mail has the same status as a letter written on official OACAS stationary.
- ✓ Make sure that the copies of received and sent e-mails are printed out and filed like other correspondence, where appropriate.

Don't

- ✗ Access the Internet for private commercial purposes
- ✗ Use e-mail to send confidential information without prior approval
- ✗ Use these facilities to access or disseminate inappropriate or illegal material
- ✗ Use anyone else's e-mail account to send e-mails

E-mail Etiquette

E-mail is like a normal letter: it is an official document of OACAS and should be treated as such. E-mail is often more immediate than the post and the temptation to not take as much care composing as with a regular correspondence means the potential for misunderstanding is high.

Do

- ✓ Make the subject line specific
- ✓ When replying to a question, copy only the question into your e-mail, then provide your response
- ✓ Address and sign your e-mails, this will prevent your e-mail from seeming abrupt and/or rude
- ✓ Read the message before you send it and consider the recipient's response
- ✓ Where appropriate, send an acknowledgement that you received the message
- ✓ Make arrangements for a member of staff to check your e-mails while you are on holiday, or absent for any length of time
- ✓ Be wary of e-mail attachments (see Virus)
- ✓ Print, date and file any significant item of e-mail
- ✓ Use the disclaimer at all times

Don't

- ✗ Use e-mail for personal use
- ✗ TYPE ALL IN CAPS
- ✗ Send inappropriate material or use e-mail to harass
- ✗ Forward any chain letters
- ✗ Use e-mail for any illegal or unethical purpose
- ✗ Rely on the privacy of e-mail

Following any complaints OACAS reserves the right to remove any message sent or received by a member of staff.

Physical Security

Do

- ✓ Be careful when eating or drinking near any computers or printers

- ✓ Ensure that you are using your workstation safely, and that the monitor and keyboard are suitably positioned
- ✓ Remember to take regular, short breaks from looking at a VDU (computer monitor)

Don't

- ✗ Leave computer equipment or other assets in a vulnerable area
- ✗ Take equipment off-site without permission
- ✗ Disclose any passwords
- ✗ Leave equipment unattended in your car