SwanCare

Policy & Procedure Manual	Information Services
Policy/Procedure Name	Information Communication Technology (ICT) Policy
Issue Date	July 2009
Last Review Date	June 2019
Authorised by	ICT Manager

POLICY

Employees at SwanCare Group may be provided with access to information systems to assist in the performance of their job duties. All ICT hardware including computers, peripherals, telephones and other such items remains the property of SwanCare Group. All software and data located on any part of SwanCare Group's networks and cloud environment, including e-mail and Internet systems is the property of SwanCare Group. Any information composed, sent or received on SwanCare computing systems are, and will remain, company property. SwanCare Group reserves the right to review, audit, intercept, access and disclose all data created, received or sent via the company's computer network.

The ICT Policy enables SwanCare Group to;

a) Ensure the security of SwanCare Group's ICT networks is not compromised and remains available for use;
b) Safeguard corporate, confidential and personal data including that which must comply with privacy legislation;
c) Ensure the ICT facilities are used by employees in an appropriate and responsible manner at all times;
d) Monitor and inspect information used and stored on SwanCare Group's networks;
e) Monitor and inspect information received or transmitted on SwanCare Group's networks;
f) Invoke disciplinary action as and when required.

1. ICT Security

1.1 Network Security

All network infrastructure equipment shall be acquired, installed, controlled, and managed by those employed in the Information Services Department or approved contractors, including, but not restricted to, routers, switches, wireless access points and any other equipment not defined above.

No personal equipment including notebooks, mobile devices, removable hard drives, USB drives or software may be connected to or installed on any device on the organisation's network or organisation's hardware without approval from the Information Services Department.

The Information Services Department may disconnect any device which is deemed to be a security risk.

Users shall not disable or attempt to circumvent security services, devices, or software on any device, nor attempt to circumvent measures that enhance information security or adherence to copyright legislation unless explicitly authorised by the ICT Manager.

1.2 Confidentiality of Information

Prior to disposal of ICT equipment owned, rented, or leased by the organisation, information (for example, information stored on hard disks) shall be securely overwritten by authorised ICT personnel to ensure that all sensitive data and licensed software have been removed.

2. Copyright, Confidentiality of Data and Privacy

2.1 Copyright

Information, software and other materials protected by copyright laws must not be copied or transmitted.

2.2 Confidential Data

All data on any of the organisation's networks or devices remains the property of the organisation and must remain on the network.

Data should only be forwarded or sent to external parties where approved by the appropriate manager.

2.3 Privacy

In order to ensure the privacy of the organisation's clients, employees and other stakeholders, users must ensure the use of any data or information on the network is maintained in a secure and professional manner.

All printed information is to be stored in an appropriately locked location and shredded upon disposal.

When a computer or device is left unattended for both short and long periods, the user should either lock the screen or log off to ensure confidentiality and privacy is maintained.

3. Usernames and Password

3.1 Usernames

All employees who require access to a computer for their job duties will be issued with a unique username and password, only to be used by that employee.

3.2 Passwords

Passwords must be set for all user accounts and must not be shared with others. Users are responsible for their user accounts and must ensure the account remains secure at all times.

A password should be a minimum of five (8) characters in length with a combination of both alpha and numeric characters. Passwords must be changed when requested. Passwords must not be recorded and must not be shared with any other staff member.

4. Appropriate Use

4.1 Transmitting and Receiving Information and other Materials

You may not use the system to view, transmit, or store any prohibited material as defined by this policy. As a general rule, employees should not include in their e-mail any communication that would not be acceptable if communicated in a public forum or access Internet sites that may offend if viewed by other staff.

Examples of internet and e-mail communication that is not acceptable include:

- Sexually or racially unacceptable messages and jokes;
- Unacceptable videos, graphics, photos, drawings and cartoons and;
- Defamatory communication.

If you receive inappropriate material, such as that outlined above, do not forward it to other employees, but immediately delete it from the system.

Employees must not use SwanCare Group's e-mail or Internet system to:

- solicit or endorse any non-job-related commercial ventures, outside organisations, or religious and/or political causes;
- send chain or spam mail in accordance with the *Spam Act 2003*;
- store or transmit information of a sensitive, confidential or personal nature;
- send information to any media outlet – newspapers, TV, radio – without managerial authorisation or;
- send, store or download offensive or defamatory material.

To maintain professional looking documentation, all e-mails should be checked for spelling and grammatical errors.

4.2 Personal Use

Personal use of SwanCare Group's e-mail and Internet system is permitted during designated break times and before/after hours only.

4.3 User Accounts

Employees are not permitted to access another user's network account without prior consent from the ICT Manager.

5. Monitoring and Inspection

SwanCare Group may at any time monitor or inspect any data which is stored or being transmitted/received within the organisation's networks.

6. ICT and security training

All SwanCare staff will complete all mandatory ICT and data security training within a timely manner.

7. Disciplinary Action

Misuse or overuse of the organisation’s network including email and Internet facilities will not be tolerated by SwanCare Group.

Any action by a staff member which compromises the security of the SwanCare network and/or results in the loss or exposure of confidential or private data, whether intentional or not may result in disciplinary action.

Appropriate disciplinary action will be taken against any employee found to have breached this policy. Depending on the seriousness of the incident this may include termination of employment.

Related Legislation: Privacy Act 1988
Copyright Act 1968
Classification (Publications, Films and Computer Games) Enforcement Act 1996 – WA
Spam Act 2003