User Responsibilities and Acceptable Use Policy

House with No Steps™

Part A: Summary

1 What is this policy and why do we need it?

1.1 The purpose of this policy is to define the responsibilities of all users of computer and telephony equipment within HWNS.

1.2 The policy also defines acceptable use (versus unacceptable use) for each category of equipment.

2 What outcomes will be achieved by implementing this policy?

2.1 This policy is designed to protect the confidentiality of sensitive information relating to all people employed, and supported by HWNS.

2.2 The policy is also designed to protect all other confidential information relating to HWNS operations by ensuring that information is made available only to those people needing access for business purposes.

2.3 By implementing this policy, confidential information will be protected from outside access and from being transmitted to external parties.

3 Who does the policy affect?

3.1 This policy relates to each and every user of HWNS information technology and telephony equipment including computers, land line telephones, mobiles, Smartphones and all aspects of the HWNS voice and data network.

3.2 This policy applies to HWNS employees, supported employees, volunteers, contractors, consultants, service providers and any other third parties.

3.3 The terms of this policy apply whether users are accessing HWNS systems remotely or locally, that is whether accessing the systems from HWNS premises or other premises. They also apply whether the user is accessing the systems using HWNS supplied equipment, or other equipment (e.g. a home computer or private Smartphone).

4 Special terms used in this policy

4.1 For a full list of QMS definitions this section should be read in conjunction with References and Definitions QMS 000 - 003.

4.2 Other terms and abbreviations used in this document include:

- Authorised: means permission or approval granted by HWNS IT&T unless otherwise stated.
- Citrix Access Gateway (CAG): is a software utility that enables remote access to the HWNS computer network.

5 Responsibilities under the policy

5.1 All users must comply with the specific responsibilities and acceptable use conditions of this policy.

Part B: Our Policy

1 Policy Statement

1.1 Computer and telephony equipment is provided by HWNS for business purposes. This equipment is used by HWNS employees, supported employees and volunteers, and occasionally by people supported by HWNS, contractors and other third parties.

1.2 Use of any equipment is subject to the user adhering to the responsibilities defined in this policy, as well the user adhering to the acceptable use provisions in the policy.

2 Access Control and Password Protection

2.1 User names and passwords are required for access to the computer network and are issued for the use of individual users only. Users may not disclose or share their password with anyone. The Citrix system will prompt users in requiring strong passwords and regular changes of passwords.

2.2 Users will not allow others to use their computer unless the others do so under their own name and password.

2.3 Users should always lock their computers (Ctrl, Alt, Del; Lock), or log out, if the computer is to be left unattended for any time.

2.4 Smartphone (PDA) users are required to use a pass-code lock for security in order to be given access to HWNS network for synchronising of email and calendar.

3 Privacy and Ownership

3.1 Users expressly waive any right of privacy or ownership of anything they create, send, receive or store using HWNS systems or networks.

3.2 Users recognise that HWNS has the right to access and review all material created, sent, received or stored on HWNS systems or networks.

4 Risks to Network, Systems Integrity and Data Security

4.1 No unauthorised computers (including users' private computers), printers, Smartphones or other devices may be physically or wirelessly connected to HWNS networks.

4.2 Private computers may be used for accessing HWNS systems, subject to EGM approval and only via an external internet link, using the Citrix Access Gateway (CAG). Call IT Support for information regarding obtaining the CAG utility.

4.3 No unauthorised software, programs or executable code may be introduced to HWNS computers, by any method.

4.4 Networks and network cabling may not be reconfigured in any circumstances, except as authorised by HWNS IT&T.

5 Acceptable Use

5.1 Use of email, access to the web and any other systems or applications should be for legitimate, HWNS approved purposes.

5.2 It is understood that a reasonable and limited amount of personal use of telephones, email and web access may occur.

6 Unacceptable and Prohibited Use

6.1 The following is a partial list of unacceptable activities. If in doubt, users should seek clarification (refer to Part B.11 of this document).

6.2 Users may not visit internet sites or display web pages containing material that might be considered offensive. Offensive material includes (but is not limited to) pornography, violence, incitement to hatred, harassment, information encouraging criminal behaviour and junk mail.

6.3 Users may not transmit material that might be considered offensive by email or by any other means.

6.4 Frivolous use, or use for personal or commercial gain, is expressly prohibited.

6.5 Users may not use equipment or transmit information in any way that is unlawful.

7 Monitoring and Logging

7.1 Users should be aware that all web access and email can be, and may be, logged and monitored by HWNS systems.

8 Care

8.1 Users should take particular care to avoid loss or theft of devices that have access to the HWNS network, particularly Laptops and Smartphones (PDAs), to minimise the risk of unauthorised access or data loss.

8.2 Users should take care to avoid the risk of introduction of viruses or malware, for example:

- never opening mail or attachments from unknown senders;
- avoiding disreputable web sites and never downloading anything from an unknown/un-trusted site; and
- never loading CDs/DVDs, or connecting memory sticks, from un-trusted sources.

9 Loss or Theft

9.1 Loss or theft of any device (especially Laptops and Smartphones) must be reported immediately to IT Support to enable arrangements to be made to secure the HWNS network against unauthorised access by those lost devices.

10 Breach of Policies; Legal Exposure

10.1 Intentional breach of any of these policies could be grounds for disciplinary action. Severe or repeated breach could be grounds for termination.

10.2 Certain breaches of policy could expose the user and HWNS to claims of discrimination, harassment or criminal behaviour, with consequences involving suspended usage, disciplinary action or involvement of police.

11 Clarification

11.1 Line management or the IT Support department should be contacted for any queries or clarification of any matters relating to user responsibilities, acceptable use or any other aspect of HWNS IT&T policies and procedures.

Part C: Procedures, tools & resources relevant to this policy

1 List of relevant QMS Procedures & Guidelines

References and Definitions QMS 000 - 003

Responsibility of Managers and Systems Owners QMS 1000 – 1007

Access and Security Controls QMS 1000 – 1008

Passwords QMS 1000 – 1009

User Support Services QMS 1000 – 1011

Assets Management QMS 1000 – 1013

Privacy QMS 000 – 004

2 Tools and Resources for implementing this document

2.1 Legislation

Nil

2.2 Forms and checklists

iMac Form 1000/0164