NHS ORKNEY

IT Security Policy

Policy Author:	**IT Manager**
Policy Owner (for updates)	**IT Manager**
Engagement and Consultation Groups:	**Information Governance Group** **eHealth Operational Group** **Partnership Forum** **Area Clinical Forum**
Approval Record	Date
Equality and Diversity Rapid Impact Assessment	
Version Control	
Version Number	**V5.5**
Date of Original Document	1 July 2008
Last Change and Approval Date	17 July 2013
Last Review Date	13 May 2013
Next Formal Review Date	1 May 2015
Location and Access to Documents	
Location of master document	IT Manager’s folder on G drive
Location of backup document	EQIA folder on G drive
Location of E&D assessment	n/a
Access to document for staff	Blog
Access to document for public	n/a
Post holders names at last review	
Tom Gilmour	IT Manager
David Rendall	eHealth Specialist

If you require this or any other NHS Orkney publication in an alternative format (large print or computer disk for example) or in another language, please contact the Clinical Safety and Quality Department:

Telephone: (01856) 888283 or

Email: ork-hb.alternativeformats@nhs.net

Index

Page

1. Foreword 4

2. Access Terms and Conditions 5
2.1. General 5
2.2. Passwords 6
2.3. Malicious software and anti-virus 7
2.4. Email 7
2.5. Fax Machines 9
2.6. Blog 10
2.7. Internet 10
2.8. Physical Security 11
2.9. Remote Access 12
2.10. Software Licensing 13
2.11. Data Protection 13
2.12. Identity Theft 14
2.13. Backing Up 15
2.14. Logging & Monitoring 15
2.15. Removable Media 16
2.16. Encryption 17
2.17. Third Parties 17
2.18. Copyright 18
2.19. SMS and Instant Messaging 20
2.20. Photography Guidance 20
2.21. Use of Personal Devices 20
2.22. Social Media 21
2.23. Scanning 21
2.24. Staff Responsibilities 22

3. Glossary 24

Appendices

Appendix 1. Equality and Diversity Impact Assessment

NHS Orkney IT Security Policy

1. Foreword

This policy applies to all employees of NHS Orkney. The term employee includes anyone who carries out work on behalf of NHS Orkney, paid or unpaid, as well as all full-time and part-time members of staff. Employees of other entities (for example general practices) who work with health data will be expected to have signed an equivalent policy modified as appropriate to their organisation.

Any employee using computing hardware and/or software belonging to NHS Orkney is expected to protect it, and the information it holds, from loss or damage. You should note that the risks are likely to be greater for equipment that is not securely safeguarded on Health Board premises.

When computers communicate with other computers, whether by email or by accessing the Internet, there are a number of risks. These risks include:

- Unauthorised people getting access to confidential information
- Programs, files, systems and information being corrupted or destroyed by malicious software
- Unlicensed software, offensive or illegal material being introduced

Any employee whose actions cause any of these to occur may be subject to disciplinary procedures, possibly leading to dismissal.

You must be aware that as an employee you are allowed to use NHS equipment only for work that is relevant to the Board's business. This includes Union-related work and professional development. Occasional and reasonable personal use is permitted provided that this does not interfere with the performance of your duties. This applies also to the use of any NHS-provided Internet access facilities. The use of these facilities within NHS Orkney will be monitored in accordance with the outlined in Section 2.14 Logging and Monitoring.

You must sign the attached statement to show that you have read and understood this policy, and agree to abide by it. The signed document must be returned to the IT Department who will ensure it is retained centrally.

2. Access Terms and Conditions

2.1. General

A glossary of technical terms can be found at the end of this document.

Note: Throughout this document, the term 'NHS Orkney computer equipment' means any hardware, software or other Information and Communications Technology (ICT) asset owned by NHS Orkney.

2.1.1. Software owned by NHS Orkney may be installed on a non-NHS Orkney computer only if:

- NHS Orkney retains the right to the software licence and there is prior authorisation by the IT Department within the terms of the relevant software license
- The user agrees to abide by this policy, as if the computer were the property of NHS Orkney, including removal of the software if requested by NHS Orkney

2.1.2. Access to NHS Orkney computer equipment will only be authorised if you have read this document and signed to agree that you will abide by its terms.

2.1.3. You must inform the IT Department if your role (or any of your direct reports roles) changes in order that permissions can be rescinded and permissions appropriate to the new role can be assigned after approval by your line manager.

2.1.4. Employees must return all ICT equipment to the IT Department when leaving the employment of NHS Orkney.

2.1.5. Using NHS Orkney computer equipment to transmit any material in violation of any UK law or regulation is prohibited. Examples of this include harassment, the transmission of computer viruses, copyright material, material legally judged to be defamatory, offensive, abusive, threatening, pornographic or obscene, and material protected by 'trade secret'. Ignorance of either the content of the material or the relevant law is not a defence in law.

2.1.6. NHS Orkney computer equipment should be used purely for work that is relevant to the Board's business. This includes Union-related work and professional development. Occasional and reasonable personal use is permitted provided that this does not interfere with the performance of your duties.

2.1.7. No software may be loaded directly onto your PC from disks, CDs/DVDs, removable media or downloaded either from the NHSnet or the Internet without written authorisation from the IT department. This includes ‘Shareware’ and other free software, games or screensavers.

2.1.8. You must not tether a laptop device to a mobile phone data connection at the same time as the laptop is connected to the NHS LAN.

2.1.9. Access to any NHS Orkney systems by remote PCs or laptops must be made only in ways authorised and installed by the IT Department.

2.1.10. All incidents which threaten the security of any NHS Orkney computer equipment must be reported immediately to your line manager and the IT ServiceDesk. The security incident must also be reported on Datix.

2.1.11. If you need advice, or wish to discuss IT Security issues in confidence, contact a senior member of the IT Department.

2.1.12. This policy will be reviewed and updated to maintain it in line with NHS Scotland Security Guidance

2.2. Passwords

2.2.1. As a user, you will be issued with a login name unique to you to access any Health Board systems. The login name will be in the format firstname.surname

2.2.2. Access to systems will only be granted with line manager, or delegate, approval

2.2.3. You must inform the IT department if you no longer require access to system(s)

2.2.4. You will be required to create a password(s) for your own use. Passwords must be kept confidential, and must be changed at regular intervals.

2.2.5. Passwords should contain a mixture of uppercase, lowercase and numerals.

2.2.6. If you believe that someone else knows your password then you must advise your line manager immediately and change your password. This must be regarded as a security incident and the IT Department advised either by completing a Datix incident form or directly, if you are concerned that it was part of a deliberate attempt to gain unauthorised access.

2.2.7. Passwords will be revoked when the user leaves employment

2.2.8. The list of main systems and how to request access is given here: ehealth1272: How to get access to computer systems

2.3. Malicious software and anti-virus

2.3.1. Approved anti-virus software must be loaded onto your computer and it must be configured to enforce the highest security possible while still allowing you to carry out your work. The corresponding virus database must be updated as frequently as possible. Contact the IT Department for assistance if you suspect the anti-virus software is not being updated or is incorrectly configured.

2.3.2. Virus protection software must not be disabled under any circumstances.

2.3.3. Any viruses detected must be reported as soon as possible to the IT ServiceDesk. Do not attempt to clean up the virus without the assistance of the IT Department. The infected machine will be isolated and cleaned as appropriate by the IT Department.

2.3.4. Information held on removable media such as memory sticks/cards, PDAs, mobile phones, firewire drives, usb drives, etc should only be connected to PCs with up-to-date Anti Virus software.

2.3.5. If you are concerned that a PC or disk has been infected, do not use it with NHS Orkney computer equipment. Contact the IT ServiceDesk immediately, who will arrange to have the equipment checked and if necessary cleaned.

2.4. Email

2.4.1. The Health Board’s email system is solely for work-related use. If your correspondence is personal, please use your own email account. (See Section 2.4 Email for guidance on accessing personal emails from the NHS Orkney network.)

2.4.2. You may only use the following email services for work-related purposes: NHS Mail, Doctors.net, email provided by professional bodies, (e.g. RCN, Chartered Society of Physiotherapists, etc) and GSX email. Circumstances where access to personal email could be withdrawn include, but are not limited to, staff spending a lot of time on their personal email and not doing their work, staff running a business from work, staff using their personal email to send work-related and patient identifiable information, etc.

2.4.3. Use of personal email accounts - e.g. Gmail, Hotmail, Yahoo, etc. - is allowed at the Board’s discretion and may be withdrawn at any time. Access is permitted only via web browser on PC/Laptop or email app on Smartphone.

2.4.4. It is possible for email to be received by individuals or organisations that are not the intended recipients. A disclaimer must be added to each email to ensure that any recipient is aware of its confidential nature and that it should be deleted if received in error. Do not use or put reliance on the contents of any email you receive by mistake.

2.4.5. Ask yourself before sending an email, how would you feel if your message were read out in court. Email messages may have to be disclosed in litigation.

2.4.6. Do not import or export any files, including email attachments, without checking them for viruses using the approved software. This includes scanned pictures or other images, live video pictures, live audio or any other items of a similar nature. If there is any doubt about the validity of the transfer you should check with the IT Department beforehand.

2.4.7. You are personally responsible for information that you transmit, either incoming or outgoing, via NHS Orkney computer equipment.

2.4.8. The contents of messages must be treated with care as they may leave the sender vulnerable to legal action in a way that normal conversation would not, and may also cause adverse publicity in the press and news media.

2.4.9. Obtain confirmation of receipt for important emails sent.

2.4.10. Archive important emails - ask the IT Department for advice on how to create an email archive.

2.4.11. Do not impersonate any other person when using email, or amend messages received.

2.4.12. Do not copy emails to those who do not need to see them. Ensure that the destination addresses are correct by using the 'Check Names' facility in Outlook and NHS Webmail.

2.4.13. If sending an email to multiple recipients use ‘Carbon Copy’ (Cc:) and consider using a distribution list.

2.4.14. Report to your line manager and the IT Department if you receive any email which you regard as illegal or offensive.

2.4.15. It is your responsibility to ensure, as far as you are able, that any information/data you send is accurate.

2.4.16. You may ONLY send patient identifiable information using an @nhs.net or @gsx address. The transmission of named patient information and other identifiable sensitive information is only permitted if both the sender and receiver use @nhs.net or @gsx addresses. However, proper precautions must still be taken. You must adhere to the provisions of the Data Protection Act, the Caldicott Guardian Code of Practice and the Email Good Practice Guide.

2.4.17. Emails sent to nhs.net email addresses must not be forwarded to personal email accounts, e.g. l ISP accounts e.g. Gmail, Hotmail, Yahoo, etc.

2.4.18. For further guidance see Email FAQs and Email Good Practice Guide

2.5. Fax Machines

2.5.1. The use of faxes should be avoided unless there is no practical alternative

- When faxing patient identifiable, confidential or staff identifiable information patients should be identifiable using the CHI number only and all demographic information should be removed from the information to be faxed
- The recipient of the fax must be contacted and told to expect a fax, the cover page should be transmitted, receipt of the cover page should be acknowledged, the remainder of the fax should be sent and receipt of the complete fax acknowledged
- Telephone numbers should be stored in fax machine to prevent faxes being sent to the wrong recipients

2.5.2. If faxing to an organisation that doesn’t have access to lookup demographics via the CHI number then all demographic details should be removed from the fax, the patient should be identified on the fax using the CHI number the fax transmitted following the fax guidelines and the demographics information sent via another channel, e.g. email or telephone.

2.5.3. For further guidance see IT3184: Fax Machine Guidance

2.6. Blog (Intranet)

2.6.1. The NHS Orkney intranet home page is a collaborative content management system, through which all notices, standards and other information is published. Individuals can also post notices.

2.6.2. All staff members are expected to use the blog responsibly, and help to maintain it as an aid to open, effective and transparent means of communication.

2.7. Internet

2.7.1. Direct Access to the Internet from any computer connected to NHS Orkney LAN is strictly prohibited. The only permitted route is through the Secure Internet Gateway via the NHSnet.

2.7.2. All connections to web services on the Internet must be made via the NHS Orkney proxy server. This includes viewing Internet content via a web browser, and also any app which connects to web services on the Internet.

2.7.3. You are required to conform to any reasonable policies, procedures and protocols of the Service Providers and any other networks or Websites that you access. If you do not conform to these your access rights to the Internet through the Internet Gateway will be removed.

2.7.4. If you use the Internet against the reasonable interests of the Board, disciplinary procedures may be invoked.

2.7.5. Information transferred via the Internet has to be seen as being in the public domain and able to be read by anyone connected to the Internet. Extreme care must be taken in using the Internet as a means of viewing or communicating information.

2.7.6. Do not deliberately visit, view or download any material from any web site containing pornographic or illegal material or material which is offensive in any way whatsoever.

2.7.7. If you accidentally connect to a web site that contains illegal or offensive information you should disconnect from the site and inform your line manager and the IT Department.

2.7.8. Advertising or any other form of promotional activity for non NHS purposes is strictly forbidden.

2.7.9. You must not create Websites or similar applications unless you have been properly authorised to do so.

2.7.10. Social media use is covered by the NHS Orkney social media protocol. For further guidance see IT4140: Social Media Protocol

2.7.11. You must not access social media sites from NHS Orkney computers unless you have been given specific authorisation to do so. This authorisation is given by line or service managers. Departments and users who wish to post to social media must have approval as per the social media protocol. See IT4140: Social Media Protocol

2.8. Physical Security

2.8.1. NHS Orkney computer equipment must not be left unattended in an insecure place at any time. It must not, for example be left unattended in a car other than in a locked boot where it is not visible to passers-by.

2.8.2. Family members are not allowed to use NHS Orkney computer equipment without prior authorisation from the IT Department. As the employee, you are responsible for ensuring that the use of the equipment is in accordance with this policy. Any suspected unauthorised use should be reported to the IT Department.

2.8.3. NHS Orkney computer equipment should be physically protected from the following, which can cause malfunctions and seriously damage the equipment and the information stored on it.

- Excessive heat, cold or humidity. Do not place equipment near a radiator or in direct sunlight.
- Dust, smoke and crumbs.
- Magnetic fields.
- Static electricity.
- Liquids (including coffee!).

2.8.4. Do not open up a PC to expose its electronic components. If the PC has a fault, call the IT ServiceDesk staff. They will arrange for authorised personnel to carry out repair or maintenance work if required.

2.8.5. Do not leave your PC when it is switched on, unless all access to it is prevented through either logon or screensaver passwords, as this could allow unauthorised people to access the data stored on it. Always switch the PC off when not in use.

2.8.6. Do not send unaccompanied PCs, PC parts or removable media by ordinary mail or air or any other transport method. If a PC needs to be transported e.g. to the IT Department for work to be carried out on it, either ensure that an employee authorised by the IT Department will be accompanying it at all times or send it by guaranteed postal service.

2.9. Remote Access

2.9.1. Staff working on home computers to gain remote access to systems must observe all the general policy guidelines on security as above, with the following added conditions to remove the possibility of any unauthorised access by members of their family or household:

2.9.2. Remote access will only be available once the associated software has been installed under the supervision of the IT department onto the machine to be used for this purpose. The software must be removed when there is no further requirement for remote access.

2.9.3. VPN tokens will be provided for sole use by the authorised person and must not be transferred to another staff member without authorisation from the IT Manager.

2.9.4. The screen must never be left on at any time when the authorised staff member is away from their desk – for however short a period.

2.9.5. The password-protected screen saver must activate after fifteen minutes inactivity, and the connection must disconnect after thirty minutes inactivity.

2.9.6. The screen settings must also be password protected with a locking mechanism to prevent data viewing if the monitor is switched on by an unauthorised person.

2.9.7. No other member of the family or household should have access to the machine during the session of use by the NHS staff member.

2.9.8. No attempt should be made to save documents held on the remote site to the local PC hard disk or any other removable disk (e.g. PDA, memory stick, etc)

2.9.9. If the VPN token is lost or damaged the member of staff will be expected to replace it.

2.9.10. No other member of the family or household should have access to the VPN token.

2.9.11. The member of staff should ensure that anti-virus software on the remote access machine is up-to-date

2.9.12. A personal firewall (standard in Windows XP and above) should be installed.

2.9.13. The IT staff of NHS Orkney must be allowed access to the pc at regular intervals for maintenance and verification purposes.

2.10. Software Licensing

2.10.1. All software used must have a valid licence.

2.10.2. No software should be loaded onto the PC without the prior authorisation of the IT Department.

2.10.3. No copies of software should be given to other users, including other staff members for use at work.

2.11. Data Protection

2.11.1. Users of NHS Orkney computer equipment must comply with the Data Protection Act and the Caldicott Guardian Code of Practice. The Director of Public Healthis the Caldicott Guardian and can provide details of the code. Any queries should be addressed to Data Protection Officer who holds the register of entries for the Health Board. The eight principles within the act are:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an

adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.11.2. The data within all centralised systems (e.g. Patient Administration) is covered by the Health Board's registration. Any developments proposed by staff which would include identifiable personal data e.g. a local database of patients, should be checked with the Data Protection Officer and the Caldicott Guardian before implementation. NHS Orkney's data protection registration may be found by clicking here and entering *Orkney Health Board* in the 'Name' search box.

2.11.3. Any computer which passes out of the ownership or control of NHS Orkney must first be securely wiped clean of any programs or data belonging to the Health Board by a member of the IT Department.

2.12. Identity Theft

2.12.1. Your personal information is valuable and attempts may be made to get it from you.

2.12.2. Do not open emails from people you don't know - delete them immediately and don't reply to them.

2.12.3. Never respond to an email supposedly from a bank - banks will never contact you by email and will always correspond by post.

2.12.4. If you are phoned and asked for personal information do not divulge it unless you can confirm the identity of the caller. If in doubt ask for a phone number to call them back on and call them back from a different phone.

2.12.5. Shred paper documents containing personal identifiable information when no longer required. See Section 2.23 Scanning for further guidance.

2.12.6. Use 'locked' printing to minimise the risk of prints being left at a printer or multifunction device and accessed by another member of staff.

2.12.7. Although NHS Orkney's IT Security Policy allows personal web-browsing NHS Orkney takes no responsibility for any personal information held on PCs which is subsequently used fraudulently.

2.13. Backing Up

2.13.1. Do not store documents and files on your local computer's disk. All documents and files should be stored on a network drive

2.13.2. Removable media must be stored in a secure place particularly if they contain confidential information. Such media must not be exposed to any of the harmful physical conditions identified in the physical security section of this document, and should not be stored in the same place as the PC to avoid loss of both disks and PC e.g. by fire.

2.13.3. No patient identifiable, confidential or staff identifiable information may be copied onto or communicated via removable / portable media, including USB sticks, smartphones and iPhones as well as any of the above, unless it is encrypted.

2.13.4. Further advice on creating backups can be obtained from the IT ServiceDesk.

2.14. Logging & Monitoring

2.14.1. The IT Department will log and routinely audit the use of all NHS Orkney computer equipment.

2.14.2. In addition to routine business monitoring the health board does reserve the right to forensically examine the contents of any device used for official business if there is a formal investigation.

2.14.3. Members of the department will treat the audit results as confidential and will not communicate their findings to anyone outside the department. If any issues or suspicions of misuse are raised by an audit check, IT Manager will report them to the user's line manager and/or Head of Department, who should take responsibility for initiating the appropriate procedures.

2.14.4. For PCs attached to NHS Orkney LAN an Internet log will record the date and time, logged in user, address of the PC workstation, address of the web page, the type of access and the name of any file accessed or downloaded.

2.14.5. Remote PC's and Laptop computers will be randomly audited to check for illegal or unauthorised software. Internet and email logs and caches on the PCs will be checked for prohibited use as detailed in this document.

2.14.6. Content auditing of emails or downloaded web pages will only be carried out if there is good reason to believe that an individual member of staff's usage contravenes criminal law, his/her employment contract, confidentiality rules, or discrimination law, or amounts to a civil wrong (such as defamation).

2.14.7. Staff may have access to any personal electronic data collected through auditing and have the right to dispute or amend inaccurate information.

2.14.8. The IT Department may take over PCs as part of their helpdesk duties, but will seek permission from the user before doing this.

2.15. Removable Media

2.15.1. The storage of confidential, staff identifiable or patient identifiable information on removable storage devices such as digital camera memory, USB storage devices, memory pens, sticks/PDAs, etc is prohibited unless all of the following conditions have been satisfied:

2.15.2. A risk assessment has been carried out by the IT Security Officer

2.15.3. The security requirements in the NHS Scotland eHealth Mobile Data Protection Standard are met.

2.15.4. Approval is given by the Caldicott Guardian for patient identifiable data or Data Protection Officer for other confidential data.

2.15.5. Patient identifiable, confidential or staff identifiable information may only be stored on encrypted devices

2.15.6. Files must be deleted from the removable storage device as soon as they have been used for their intended purpose. Permanent copies should be stored on network drives only.

2.15.7. Removable storage devices should be returned to the IT department for secure disposal when no longer required.

2.15.8. For further guidance see Mobile Data Standard FAQs and Mobile Data Standard

2.16. Encryption

2.16.1. NHSO will encrypt laptops provided by NHS Orkney and, where permitted, laptops provided by other partner agencies

2.16.2. Patient identifiable, confidential or staff identifiable information belonging to NHS Orkney must not be held on a personal computer or unencrypted laptop (This applies whether the machine is owned by the individual or by NHSO).

2.16.3. If an encrypted laptop remains unconnected to an NHS Orkney LAN for an extended period the laptop may be locked and will have to be returned to the IT Department for unlocking

2.16.4. Encrypted devices used to store patient identifiable, confidential or staff identifiable information must be approved by the IT Manager

2.16.5. Usernames and passwords used with encrypted devices must consist of a mixture of lowercase, uppercase and numerals

2.16.6. Usernames and passwords used with encrypted devices must not be given to other users

2.16.7. NHSO will not encrypt personal laptops. By personal laptops we mean laptops which are the personal property of staff, not laptops provided by NHSO.

2.16.8. No attempt should be made to bypass the encryption

2.16.9. For further guidance see Mobile Data Standard FAQs and Mobile Data Standard

2.17. Third Parties

2.17.1. The minimum information only shall be divulged to third-parties.

2.17.2. When sending documents, etc ensure that additional information has been deleted from the document and that all revisions and changes to the document have been removed. If you are unsure how to do this contact the IT ServiceDesk

2.17.3. Patient identifiable, confidential or staff identifiable information must be encrypted before being sent to third-parties

2.17.4. The encryption shall be at least 256-bit AES encryption. Contact the IT ServiceDesk for advice on how to do this

2.17.5. The encryption key shall be a random sequence of at least 12 characters long and should consist of at least one uppercase character , one lowercase character and one number.

2.17.6. The encryption key shall be passed to the third party by a different means to the data (e.g. if the data has been emailed to the third-party the encryption key must be given to the third party via telephone, or SMS text message)

2.17.7. The secure file transfer site https://nww.sft.nhs.uk/sft/upload1 should be used where possible to transfer patient identifiable, confidential or staff identifiable information. Note this site is only accessible from within the NHS.

2.17.8. For further guidance see IT4169: Confidentiality Agreement for Third Party Suppliers Protocol

2.18. Copyright

2.18.1. Always put yourself in the position of the copyright owner. Copyright is not the right to copy; it is the right to prevent third parties from copying material (including scanning) without permission from the copyright owner.

2.18.2. NHS Scotland policy is that third party materials should not be copied or scanned under the 'fair dealing' or library privilege exceptions to copyright

2.18.3. As a general rule do not photocopy or scan from print publications protected by copyright - e.g. from books. journals, reports, etc

2.18.4. Journal articles should be sourced in electronic form from the Knowledge Network wherever possible. These online resources are licensed for use in NHS Scotland

2.18.5. Copyright legislation also covers electronic media, including images, photographs, logos, maps, films, videos, radio and TV broadcasts, etc. Note that websites are also covered

2.18.6. Always check the copyright disclaimer before copying

2.18.7. If an item is not available electronically and a photocopy is essential contact the Learning and Development Department

2.18.8. Some items have a HIGH risk of copyright infringement and a license or other explicit permission must be sought when using images, photographs, logos, maps and web links for the following.

- Anything copied for educational or training purposes except for examination purposes

- Anything published on the Web, or to a large group of people on an Intranet (e.g. the blog)
- Anything shown in public, e.g. in public spaces such as a hospital or health centre or public events
- Any revenue-generation activity
- The use of anything that is commercially available e.g. journal articles, music (including radio broadcasts), films, books, broadcasts, magazines, software.

2.18.9. Some items have a LOW risk of copyright infringement and should be able to be used, but check beforehand:

- Material created by staff which does not incorporate any third party materials
- Material with Creative Commons or other explicit permission, as long as the license conditions are observed. Permission must be given in written form, evidence of having been given permission to copy must be retained and the source must be acknowledged. Click here to access Creative Commons
- Anything out of copyright. It is reasonable to assume anything published that is over 120 years old is out of copyright.
- Examination, judicial proceedings and 'fair-dealing' (restricted to students and members of the public)

2.18.10. When using web links note that:

- Placing a link to the URL (web address) of a home page is not breach of copyright
- Providing a link and short title or name of other web site is not breach of copyright, but using a long title might be
- Providing a link, title and text may be breach of copyright
- Providing a link to a URL within a website (i.e. 'deep-linking') should be avoided. Instead link to the home page then give directions to the URL.

2.18.11. For further guidance see Copyright Guidance Part A and Copyright Guidance Part B

2.19. SMS and Instant Messaging

2.19.1. SMS (text) Messages should be kept short and ideally be restricted to fewer than 20 words

2.19.2. Never copy and paste an entire email into an SMS or Instant Message (IM)

2.19.3. Keep the SMS simple

2.19.4. Always enclose a contact number or email address

2.19.5. Obtain patients' consent before sending them SMS or IMs

2.19.6. Use distribution list to ensure the message is sent to the correct person

2.19.7. Keep personal information transmitted via SMS or IM to a minimum

2.19.8. For further guidance see SMS Good Practice Guide and SMS Risk Assessment

2.19.9. **Photography Guidance**

2.19.10. The express permission of individuals must be obtained when filming or photographing individuals or groups, when it is possible to identify that individual.

2.19.11. They must also be informed of the reasons for taking the film or photograph and how and where the image(s) will be used.

2.19.12. Extreme care must be taken where the picture has been taken with a smartphone to prevent the picture being forwarded onto an email address or social media site.

2.19.13. For further guidance see IT4183: Photography Guidance

2.20. Use of personal devices ('Bring Your Own Device' / BYOD)

2.20.1. NHS Orkney reserve the right not to allow the use of personal devices on the NHS Orkney network

2.20.2. If you chose to use your own device for a business purpose you will need to have the relevant business and security applications downloaded onto it; to understand that in event of the device being lost the data will be wiped and in exceptional circumstances the board may need to forensically examine the device

2.20.3. Line manager approval should be given before a personal device is used on the NHS Orkney network

2.20.4. Use of personal devices should not interfere with the performance of your duties

2.20.5. The use of 'Apps' may be disabled when connected to the NHS Orkney network

2.20.6. Storage of data on personal devices must conform to the NHS Scotland mobile data protection standard guidance

2.20.7. Any suspected breach of this guidance may result in the device being reset to factory default settings

2.20.8. Use of personal devices is entirely at the owner's risk. If the device is damaged while being used for NHSO duties, NHSO will not repair or replace it.

2.21. Social Media

2.21.1. Staff may access NHS Orkney social media sites (e.g. Facebook), BBC Radio Orkney social media sites (Facebook and Twitter), and Orkney Islands Council social media sites (Facebook and Twitter).

2.21.2. Access is granted to these sites on a view-only basis primarily for the purpose of weather and travel information. Staff should not use these sites as a gateway to other social media sites and should not publish to these sites unless they have gone through the approval process.

2.21.3. NHS Orkney staff may publish to social media sites in support of their role and where there are clearly defined benefits to NHS Orkney, its patients and stakeholders. Publishers must have permission to do so from their line manager, and must have completed an Authorisation Form and Process approved by their Director.

2.21.4. For further guidance see IT4140: Social Media Protocol

2.22. Scanning

2.22.1. Scanned documents must adhere to the British Standard BSI DISC PD0008 (or BSI BIP0008) – 'Legal Admissibility and Evidential Weight of Information Stored Electronically' and BSI PD0016:2001) 'Document Scanning: Guide to Scanning Business Documents'

2.22.2. Paper documents must only be scanned using equipment which has been approved by the IT department.

2.22.3. Paper documents should not be scanned where an electronic version is already available.

2.22.4. Before scanning, documents should be removed from binders, staples and paper clips should be removed and documents should be unfolded or unrolled as necessary. Documents should be put back in their original form after scanning if paper copies are to be retained.

2.22.5. After scanning check that all documents have been scanned by reconciling the number of images with the number of scanned sheets.

2.22.6. The quality of the image should be checked, by checking the first and last images in the batch.

2.22.7. Once the documents have been scanned they should be stored on network drives and indexed to aid retrieval. Indexing can consist of date of scan, demographic information, name and address of sender (if a letter). Indexing should be as consistent as possible to facilitate retrieval.

2.22.8. Paper documents should not be destroyed until the scanned copies have been verified, and should be disposed off securely, e.g. by shredding.

2.22.9. For guidance on document retention, see Management994: Records Management Policy

2.23. Staff Responsibilities

2.23.1. You must be aware of your responsibilities under:

- The Data Protection Act 1998
- The Computer Misuse Act 1990 with regard to unauthorised access to computer systems and the deliberate transfer of viruses and other malicious code.
- Copyright Design and Patents Act 1988 with regard to the copying of protected material including software.
- Freedom of Information (Scotland) Act 2002 with regard to the openness of information
- Protecting Patient Confidentiality NHSScotland Code of Practice
- NHS Scotland Information Assurance Strategy CEL 26 (2011)
- NHS Scotland Mobile Data Protection Standard CEL 25 (2012)
- NHS Orkney IT Security Policy (this document)

- NHS Orkney Mobile Communications Devices Criteria and Policy
- NHS Orkney Photography Guidance

If you are uncertain of these responsibilities contact the IT Security Officer, Data Protection Officer or Caldicott Guardian for further information.

IT Security Officer:	David Rendall
	mailto: david.rendall@nhs.net
	Tel: 01856 88 8157
Data Protection Officer:	Tom Gilmour
	mailto:tom.gilmour@nhs.net
	Tel: 01856 88 8055
Caldicott Guardian:	Dr Louise Wilson
	mailto: louise.wilson2@nhs.net
	Tel: 01856 88 8044

3. Glossary

Email - the name given to electronic mail messages sent between computers for named individuals or groups of individuals. Email can be collected by the appropriate person by quoting their ID and password from any computer connecting to NHS Orkney LAN NHSnet and Internet Services.

Encryption -converting information using a code that prevents it being understood by anyone who isn't authorised to read it.

Guidance on Passwords - Many users will opt for passwords that they find particularly easy to remember. Often the password chosen has strong associations with either the system being accessed or the background of the user and can be guessed by potential intruders. A strong temptation when several people share a password is to use the application name (e.g. **PAYROLL**).

- Passwords must consist of a minimum of 6 characters, at least one of which should be a non-alphabetic character.
- Passwords must not relate to the system being accessed.
- Passwords must not relate to the user. e.g. name, family names, house name, car type etc.
- *One way of creating a password meaningful to the user but not easily guessed by anyone else, is to choose a phrase and compose the password from the initial letters and numbers of the words. For example,*
- "**ILIA2BH**" - **I L**ive **I**n **A 2 B**edroomed **H**ouse
- "**IGOH28J**" - **I G**o **O**n **H**oliday **28**th **J**une
- **"MTNBW62" - M**y **T**elephone **N**umber **B**egins **W**ith **62**
- *Or:*
- *Linking two words together with a non-alpha character. For example, "**CAT*FOOD**" or "**BELL%BOOK**"*
- *Forming easy to remember anagrams of words or names and adding a non-alpha character. For example, "**NAILGIL***" (GILLIAN*) or "**ARDHOW£"** (HOWARD£).*
- *Replacing letters in a word or name by a non-alpha character. For example, "**CHA#LE*"** (CHARLES) or "**CAR&OON**" (CARTOON)***ID** - Identifying code name

NHSnet - is a private network (Intranet) for the NHS.

NHS Orkney LAN - is an internal private network for NHS Orkney providing communication within the Board. It also gives a route for secure communication between NHS computers using the NHSnet and can act as a secure method of accessing the Internet.

Internet - the global data communications network which utilises telecommunications technology to connect thousands of computers.

PC - any desktop, deskside or portable personal computer

PUBLIC DOMAIN - access is easily available to the world at large.

Services - access to the Internet using a Service Provider (e.g. CompuServe).

Transmission - The sending of information/data using NHS Orkney LAN and/or Internet Services.

Website - information on a computer that can be accessed and interrogated. This information is kept up to date by the person who manages the website. There are often areas called 'bulletin boards' that allow users to 'post' notices that can be read by other users of the site.

NSS - National Services Scotland

Viruses - the common term for a collection of different types of malicious code that has been deliberately designed to copy itself onto different types of computer media causing alarm and, in some cases, damage to the data held on computer systems. Viruses are not normally detectable until they start to cause problems. The problem is so serious that several different brands of software have been developed to detect and destroy these viruses. The best protection is gained from using anti-virus software that has a good reputation and is regularly updated.

VPN – Allows secure access from internet to corporate network (e,g, NHS Net)

Appendix 1:

NHS Orkney – Equality and Diversity Impact Assessment Rapid Impact Checklist: Summary Sheet Document title: Information Technology Security Policy	
Positive Impacts (Note the groups affected) • Sets out clear guidance for all NHS Orkney staff (including anyone who carries out work on behalf of NHS Orkney, paid or unpaid, as well as all full-time and part-time members of staff and Employees of other entities for example general practices) on use of ICT equipment • Pulls together all guidance within one document eg Data Protection, photography, social media for ease of reference	**Negative Impacts (Note the groups affected)** No negative impacts identified.
Additional Information and Evidence Required None required.	
Recommendations None required	
From the outcome of the RIC, have negative impacts been identified for race or other equality groups? Has a full EQIA process been recommended? If not, why not?	

Names and Signature(s) of Level One

Impact Assessor

Jean Aim Jean Aim

Date : 5 July 2013