University Hospitals of Derby and Burton NHS Foundation Trust

TRUST POLICY AND PROCEDURES FOR THE USE OF INTERNET AND EMAIL (INCLUDING ACCESS VIA MOBILE DEVICES) – RDH and LRCH Sites Only

Reference Number	**Version** 2.2		**Status** Draft	**Author:** Mark Chester **Job Title** Head of IT
Version / Amendment History	Version	Date	Author	Reason
	1	2008	D. Seaton	Original policy
	2	2010	D. Seaton	Review and reformat
	2.1	April 2014	D. Seaton	Review and amendments
	2.2	Nov 2018	M Chester	Interim update pending IT services merger.
Intended Recipients: All Trust staff, visiting staff from other organisations, employees of temporary employment agencies, third party users and contractors.				
Training and Dissemination: Training and awareness provided at regularly arranged IT training sessions. Dissemination via the Trust Intranet.				
To be read in conjunction with: Trust Information Governance Policy; Trust Policy for Data Protection and dealing with confidential information; Trust Policy and Procedure for Information Technology Security; Trust Disciplinary Policy; Trust Staff Guide to Information Management and Technology Security; Trust Policy and Procedures on Dignity at Work; Trust Policy on Fraud; Trust Policy for Records Management, Trust Retention & Destruction Schedule.				
In consultation with and Date: IT Management Team; Information Governance Team, Human Resources, East Midlands NHS Local Counter Fraud Services, Information Governance Action Group, Information Governance Steering Group.				
EIRA stage one Completed Yes Stage two Completed N/A				
Approving Body and Date Approved			Information Governance Steering Group – Decemnber 2018 TOG -	

Date of Issue	December 2018
Review Date and Frequency	November 2019

Contact for Review	Head of IT
Executive Lead Signature	Director of Finance and Information/SIRO
Approving Executive Signature	Executive Medical Director/Caldicott Guardian

Contents

Appendices

TRUST POLICY AND PROCEDURES FOR THE USE OF INTERNET AND EMAIL (INCLUDING ACCESS VIA MOBILE DEVICES)

1 Introduction

This policy only applies to the following sites of University Hospitals of Derby & Burton NHS Foundation Trust:-

- ***Royal Derby Hospital***
- ***London Road Community Hospital***

For all other sites, until the insourcing of IT Services is completed, please refer to the following policy:

- ***Information Security Policy V7 February 2017***

University Hospitals of Derby & Burton NHS Foundation Trust (Royal Derby and London Road Community Hospital sites) (is obliged to abide by all relevant UK legislation. This requirement devolves responsibility to the employees and agents of the Trust, who may be prosecuted, if found to be in breach of any of the following acts. Three main laws apply – the Data Protection Act (2018), the Copyright, Designs and Patents Act (1988), and the Computer Misuse Act (1990). In addition, the Caldicott Report – which centers on the protection and use of Patient Information – has a particular bearing on the way in which information can or cannot be used. For more information see Trust Information Governance Policy and Trust Policy & Procedure for Information Technology Security.

University Hospitals of Derby & Burton NHS Foundation Trust (Royal Derby and London Road Community Hospital sites) provides Internet and email access primarily for business purposes.

High-profile incidences regarding security of personal and sensitive information emphasise the need for all members of Trust staff who access the Internet and the email systems to be mindful of any actions that could jeopardise information security.

Due to the open nature and ready availability of email and Internet services, including access via mobile devices, there are potential dangers associated with its use. The Internet and email are the most common source of computer viruses, malware, spyware and other malicious code. Infected files could be unwittingly downloaded from the Internet, or contained in email attachments. These could arise from malicious intent, carelessness, complacency or misuse.

2 Purpose and Outcomes

The purpose of this Policy and Procedures is to clearly define the acceptable use of Trust Internet access and NHSMail, and to ensure the security of the email system, and the information transmitted, particularly sensitive information. It will also ensure that all staff are aware of what is deemed as acceptable and unacceptable.

The outcomes are to:

- Ensure availability – ensure that the network and email system is available for users.
- Preserve integrity – protect the network and email system from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets
- Preserve confidentiality – Protect assets against unauthorised disclosure

By following the guidelines set out in this Policy and Procedures, the Internet and email user can minimise the legal risks involved in the use of the systems. Failure to comply with the requirements of this policy will result in disciplinary action being taken. Although each case will be judged on its merits, misuse of the internet/email

(or any misuse of computer systems) may be considered Gross Misconduct and lead to dismissal.

3 Definitions Used

Defamation & Libel	A spoken or written statement or series of statements that affects the reputation of a person or an organisation. If the statement is not true then it is considered slanderous or libelous.
Harassment	Bullying and harassment is based on the complainant's perception of the situation. For further information regarding definitions of harassment see the Trust Policy and Procedures on Bullying and Harassment in the Workplace.
Proxy	A method by which an individual can provide limited access to their mailbox and/or office diary to allow colleagues to read and sometimes reply to messages and diary appointments. All persons accessing a colleague's mailbox and/or office diaries do so by use of their own user ID and password.
TARS Database	TARS is primarily used within IT Services to record, monitor and report on staff training and demographics. It provides a complete record of all training undertaken, systems to which staff have access and their designated access level, courses run within the trust (including the ability to schedule and maintain these) and allows trainees to be booked onto courses.

4 Key Responsibilities/Duties

4.1 Caldicott Guardian

The Caldicott Guardian must approve all procedures that relate to the use of patient and service-user information and is responsible for enabling appropriate information sharing.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is the executive lead and is responsible for ownership of information risk across the Trust. The SIRO acts as advocate for information risk on the board and provides written advice to the accounting officer on the information content of their Statement of Internal Control in regard to information risk.

4.3 Director of Informatics

The Director if Informatics is responsible to the Trust Board for ensuring that the Policy and Procedures for the Use of Internet and Email is being effectively implemented and communicated and that appropriate staff training is in place.

4.4 Management Responsibilities

Line Managers are responsible for dealing with any concerns raised by staff regarding this Policy and Procedures. They must liaise with the IT Services, the Information Governance team and Human Resources Departments with regard to breaches of this Policy and Procedures.

4.5 IT Services and Human Resources Department

Further monitoring and investigation of any suspected breaches of this Policy and Procedures will be carried out by the IT Services and Human Resources Department. If evidence shows that this Policy and Procedures has been breached the Human Resources department will advise on any disciplinary action necessary.

4.6 IT Directory and Email Support Officer

The IT Directory and Email Support Officer oversees the administration of the email system.

4.7 Local Organisation Administrator (LOA)

The LOA can be contacted via the IT Service Desk and provides help and support with any issues relating to the NHSmail system.

4.8 Head of Information Governance

The Head of Information Governance is responsible for monitoring and investigating suspected breaches of the Data Protection Act or Caldicott Principles.

4.9 Information Governance Steering Group

The Information Governance Steering Group is chaired by the Caldicott Guardian and reports to the Management Executive. The group is attended by the SIRO and representatives from IT Services, Information Governance, Information Services, and Records Management. Any information security issues will be highlighted here for relevant assessment and action.

4.10 All Trust Staff (Royal Derby and London Road Community Hospitals Sites only)

Individuals are granted access to the Trust's Internet and email systems on the understanding that they abide by this Policy and Procedures, the NHSMail Acceptable Use Policy (See Appendix 1), and are aware of the consequences of any breaches. Staff should raise any concerns regarding misuse of the Internet and email facilities with their manager.

5 Implementing the Policy and Procedures for the Use of Internet and Email (Including Access via Mobile Devices)

Anyone wishing to access the Internet and open an email account must complete a request form and contact the IT Service desk to arrange for an account to be activated.

All access to the Internet and Email Systems is recorded on the TARS Database and access is removed when staff leave the Trust, in accordance with Trust IT Security Policy and IT Operations Procedures.

5.1 Acceptable Use of Internet Access

Internet connectivity is provided to facilitate a person's work as an employee or student at this Trust, specifically in terms of clinical, educational, training and research. Access is also encouraged to facilitate and improve health service management activities. Commercial work is unacceptable. All internet access is monitored by IT services.

Employees must not access the internet for personal use during their working hours. Recreational use of Trust Internet access is limited to lunch breaks, work breaks and periods outside their working day. There are a number of PC's located within the internet café and the library for staff who do not have access to a PC.

While personal use of the internet is permitted during lunch and work breaks, this is only providing that the material accessed is appropriate and not potentially offensive to others. Employees should regard this facility for personal use as a privilege that is only exercised in their own time, without detriment to their job, or the work of others and not abused. Any personal details are entered at your own risk – i.e. details entered for internet banking, shopping or any other site where you enter your own details.

Inappropriate use of the internet, including violation of this policy, will result in disciplinary action being taken and/or removal of facilities.

5.2 Unacceptable use of the internet:

- Accessing of pornographic and abusive or offensive material, including sites that may constitute unlawful discrimination on the grounds of race, disability or gender, is not permitted. Such actions will be regarded as gross misconduct and will result in disciplinary action being taken.

- Work related information must not be included in postings to blogging and social networking sites. For more information please see Trust policy & procedure for the use of social networking sites.

- Any attempt to bypass security and control measures will be regarded as gross misconduct.
- Downloading software from the internet without authorisation from the IT Services Department. This excludes information files from NHS related sites

- Software and/or hard copies of data that becomes available through the use of computing or communications equipment must not be copied or used without permission from the licence holder (publisher).

- The Trust must not be committed to either legally or contractually on any website unless the individual has been authorised to do so by the Director of Finance and Information.

Any of the above will lead to disciplinary action being taken and/or the withdrawal of service for the individual concerned.

Information Security cannot be guaranteed on the Internet. Staff must consider the Internet to be in the public domain. Personal details are entered at your own risk.

5.3 Acceptable Use of Email

The email system used by Derby Hospitals is NHSMail. The full NHSMail Acceptable Usage Policy can be found at Appendix 1. Like the Internet, there are many risks as well as benefits associated with the use of email systems. This section of the Policy and Procedures seeks to ensure that email is used as securely as possible, whether on Trust PCs or via mobile devices (See Appendix 2 for email and mobile devices).

Emails must be regarded as "documents" disclosable in litigation (legal proceedings), even if they have been deleted from the recipient's in-box. If a computer's hard drive, or server, has retained a copy of the email then this must be disclosed. Where an issue arises as to the actual receipt of an email or its timing then it may be necessary in litigation to inspect the computer's hard drive.

Emails are also subject to the provisions on the Data Protection Act 1998 and the Freedom of Information Act 2000. This means that emails may have to be disclosed to individuals or outside agencies.

There is an inherent danger with emails as a means of communication. Staff may

be tempted to exercise less caution than in paper communication, believing that email communication is informal and temporary.

NHSMail

National recommendations state that there should be **No** electronic transfer of unencrypted Person Identifiable Information across the NHS. This is the default position to ensure that patient and staff personal data are protected. Therefore Derby Hospitals will provide all staff with an NHSMail account. There are three ways to access nhsmail

- Through Microsoft Outlook client
- Through the NHSmail web browser
- Via a mobile phone/tablet.

NHSMail has been specifically designed with the needs of the NHS in mind and enables staff to exchange personal and sensitive data for both staff and patients securely. It has been endorsed by the British Medical Association, Royal College of Nursing and Chartered Society of Physiotherapy. However, users must play their part in ensuring that they handle personal and sensitive data the correct way when using NHSMail.

NHSMail (nhs.net) to NHSMail is secure. NHSMail to nhs.uk email address is NOT a secure route and personal/sensitive data is at risk if sent this way without additional protection. NHSMail is part of the Government Secure Intranet, as secure network for public sector organisations (police, local and central government and criminal justice services). For more information see Appendix 3.

5.4 Transfer of personal/sensitive data

One of the biggest risks to the security of persona/sensitive data is human error. There will be people, who may have the same name, sometimes in the same organisation, you must be sure that the email address you are sending to will be received by the right person. All users are responsible for ensuring that they are emailing the right person. Where necessary send an email asking the user to confirm their identity before you send any personal/sensitive information.

Always make sure that any exchange of personal/sensitive information is part of an agreed process. Both the sender and the recipient should know what is to be sent, what it is for and how it will be used. For further advice please contact the Information Governance Manager on ext 88646

Caldicott principles should apply whenever sensitive information is exchanged.

5.5 Offsite/Home working

NHSmail may be accessed using non Trust PCs via a web browser on an internet connected PC/other device or on phones that are permitted to be used on NHS Mail (e.g Android 4.0 and above or IPhone 4 and above – these will force encryption). To maintain security of NHSmail these PCs must be protected by an up-to-date anti-virus programme and a personal firewall. Personal and sensitive information must not be accessed using a non Trust PC. If it is necessary to work with personal and sensitive information from a location other than Trust premises, an encrypted

Trust laptop must be used. Refer to Policy and Procedures for Mobile Computers and Removable Media (including Remote Access) for further information.

If an NHSmail account is being accessed via a non-NHS connection, users will be asked to specify whether or not a public/shared or private computer is being used during the login process. If a public computer is being used (i.e. in an internet café) the user will be prevented from downloading and saving email attachments. If the user selects 'private' then they will be able to download and save attachments, however the Trust does not recommend that personal and sensitive information be accessed using a non Trust PC.

5.6 Staff who transfer from this Trust to another NHS Trust.

All staff who transfer to another NHS organisation must ensure that all emails relating to the business of Derby Hospitals Foundation Trust are either deleted or transferred to an appropriate mailbox or archived within this organisation. Emails relating to the business of Derby Hospitals Foundation Trust must not remain in the inbox when an individual leaves this Trust.

5.7 Unacceptable use and risks associated with emails

- Sending or forwarding emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the Trust can be held liable.
- Sending an attachment that contains a virus, you and the Trust can be held liable.
- Forwarding a confidential message without acquiring permission from the sender first.
- Sending unsolicited email messages.
- Forging or attempt to forge email messages.
- Sending email messages using another person's email account, unless permission has been granted.
- Breaching copyright or licensing laws when composing or forwarding emails and email attachments.
- For any private commercial activities (e.g. running a business)
- Any form of defamation, discrimination, harassment or bullying.
- To bring the organisation or a colleague into disrepute
- Where it interferes with the work of the individual, a colleague, or the department.
- Where it interferes with the business of the organisation
- Subscribing to non work related forums using your work email address.
- The automated forwarding of NHS emails to public Internet email addresses.

5.8 Automated forwarding

It is not possible to auto-forward from NHSmail to an external email address. Auto forwarding is only permitted to other NHSmail users and to secure government domains (see appendix 1, 4.1)

5.9 Security

All password and log in details for email systems must be kept confidential.

The NHSmail team and HSCIC will never send out emails asking for passwords. This information should be kept confidential. Any emails asking for such information should be reported to the IT Service desk. Do not reply or click on any link in the email. Never click on a link or open an attachment that has been sent from an un-trusted source. Delete any email containing links or attachments if you do not know the sender. This will also ensure protection against the risk of virus infection.

No member of IT Services, or any member of staff, would ask individuals to download anything from websites or via an email link. It is important that no information regarding usernames, passwords or any other details are given out either on the phone, via an email or in person.

Users must inform IT Services immediately if they suspect a virus issue has occurred. If a department knowingly contravenes this part of the Policy and Procedures, the Trust reserves the right to charge part, or all, of any cleanup costs to that department.

The recipient of a sensitive email must ensure that any clinical information sent conforms to the Caldicott Principles.

5.10 Transmission of large files

The transmission of very large files on the Internet and NHSmail should be avoided. On the NHS N3 network, file sizes should be less than 10 Mb and on the Internet, this should be reduced to 2 Mb. File compression such as WinZip and other file transmission protocols (FTP) should be considered for large files. Remember the recipient of the file may have restrictions set for large files.

5.11 Right for employers to intercept emails (and phone calls)

The Trust reserves the right to monitor the content of all email transmissions, telephone calls, voicemail and Internet access for Information Security purposes.

The Trust can only access email accounts if authorisation from the user is granted or via HSCIC for forensic search, i.e. HR, criminal or clinical.

5.12 Attachments

It should be noted that encrypted attachments are blocked by the NHSmail service, to avoid the risk of computer viruses being sent or received (Appendix 4). Any attempts to bypass encrypted security controls in NHSmail must be avoided. The NHSmail antivirus software will remove encrypted attachments, but should an encrypted attachment bypass the antivirus software, subsequent automatic detection updates will automatically remove the attachment of an historic item.

Any attachments containing sensitive information should be saved to a secure location within the Trust Network. NHSmail is not designed to be a long term information store. NHSmail (as with other email systems) should only be used for the purposes of transporting information.

Users should also be aware that when an attachment is opened, a copy will be saved to the temporary internet files drive in the computer and will remain there until the cache is cleared. Therefore personal and sensitive information must not be accessed using a non Trust PC.

5.13 Email communication of clinical information

Staff must not send clinical information as an email unless it is part of an approved process between Health Care Professionals who have agreed to such an exchange. The agreement must be documented as a procedure and approved by Information Governance and IT Services (Appendix 6).

5.14 Generic Email Accounts

All requests for generic email accounts should be made via the IT Service desk. Generic accounts will be created by the Trust as authorised by the NHSMail Local Administrator.

These accounts must only be used for the purpose intended and all staff must be trained and made aware of the reason for these accounts and must notify the IT Service desk when access is no longer required.

A generic NHSmail account must be used to send and receive sensitive emails on a regular basis (See Section 5.5). Authorised users of generic accounts must ensure that local policies and procedures are in place to protect privacy and confidentiality of all personal and sensitive information. Such sensitive information includes all Patient Identifiable Data.

5.15 Proxy Access

If a user is aware that they will be away from the work environment for a long period of time (e.g. maternity leave) they must ensure that their email account is set up to allow relevant colleagues to have proxy access. This will ensure that important communications are acted upon during the user's absence.

If access is required to the account of a user who is unexpectedly on long-term leave the user's Line Manager, or a Senior Manager, must make a request for proxy access using the Request for Full Proxy Email Access form, which is available on the Intranet or via IT Service desk.

5.16 Training

The Trust will ensure that all users are properly trained before using the Internet and email system.

The Trust will take all reasonable steps to ensure that users of the email service are aware of policies and procedures and the legal obligations relating to the use of Internet and email. This will be done through training and staff communications at departmental and Trust-wide levels.

6 Monitoring Compliance and Effectiveness

Monitoring Requirement:	Contents of emails to ensure that these Policy and Procedures are adhered to. Internet usage: • Time spent on the Internet • List of visited websites. Logs of Internet usage are used to investigate allegations of misuse. Malicious code attempts.

Monitoring Method:	This is not routinely monitored. However, the Trust reserves the right to retain message content as required to meet legal and statutory obligations. If there is evidence that any member of staff is not adhering to the guidelines set out in this Policy and Procedures, the Trust reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action. Responses and details of malicious code attempts reported via IT Service desk calls recorded on spreadsheet.
Report Prepared by:	Support Services Manager / Technical Services Manager
Monitoring Report presented to:	Information Governance Steering Group (as part of Toolkit monitoring) – locally, to Investigating/Disciplinary Team.
Frequency of Report:	Quarterly (as part of Toolkit monitoring) – locally, reports produced upon request.

7 References

NHS Care Records Guarantee (2009)

BS ISO/IEC 27002:2005

BS ISO/IEC 27001:2005 BS7799-2:2005

Department of Health (2007) Information Security NHS Code of Practice

NHS Connecting for Health Good Practice Guidelines in Information Governance – Information Security

NHS Connecting for Health (2006) Good Practice Guidelines: Email, Calendar and Messaging Services

NHSmail Guidance Pages:
https://web.nhs.net/public/InformationGuidanceServices/DefaultPage.aspx

ICO (2003) The Employment Practices Code – Supplementary Guidelines: Good Practice Recommendations – Part 3: Notes and Examples – Monitoring at Work

Department of Health Informatics Directorate (2009) NHS Information Governance: Information Risk Management – Guidance: Blogging and social networking

Appendix 1

NHSmail Acceptable use policy

1. About this document

This document explains how the NHSmail service should be used. It is your responsibility to ensure that you understand and comply with this policy. It ensures that:

1.1. You understand your responsibilities and what constitutes abuse of the service

1.2. Computers and personal data are not put at risk

If you have any questions about these terms and conditions, you should contact the NHSmail team at: feedback@nhs.net

The NHSmail team reserves the right to update this document as necessary. A copy of the current version can be found at: http://www.nhs.net. Click 'Search Directory' and the Acceptable Use Policy (AUP) can be seen in the bottom left hand corner of the screen. (An NHS/N3 connection must be used).

Supporting information can be found via the NHSmail Training and Guidance pages at https://web.nhs.net/portal/InformationGuidanceServices/DefaultPage.aspx when logged into your account.

2. General information about the NHSmail service

2.1. The NHSmail service has been provided to aid the provision of health and social care and this should be your main use of the service. There may be circumstances under which it is necessary for a designated and authorised person other than yourself to view the contents of your files and folders within NHSmail, for example if you have a secretary or PA that organises your diary

2.2. If you are a member of clinical staff you may use the NHSmail service in relation to the treatment of private patients in accordance with your own professional codes of conduct

2.3. HS staff contact details are provided in the NHS Directory to support the delivery of healthcare - these details will be shared across the NHS

2.4. All data retained within the service remains the property of the NHS

2.5. NHSmail accounts are owned by HSCIC on behalf of the Secretary of State for Health and provided to NHS staff for their use

2.6. The NHSmail programme reserves the right to withdraw an email account from use should operational requirements dictate

3. Your responsibilities when using the service

3.1. General responsibilities:

3.1.1. You must not use the NHSmail service to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for immediate dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Use of the service for illegal activity will result in the immediate suspension of your NHSmail account

3.1.2. You must not use the NHSmail service for commercial gain. This includes, but is not limited to: unsolicited marketing, advertising and selling goods or services

3.1.3. You must not attempt to interfere with the technical components, both hardware and software, of the NHSmail system in any way

3.1.4. When you set up your NHSmail account you must identify yourself honestly, accurately and completely

3.1.5. You must ensure your password and answers to your security questions for the NHSmail system are kept confidential and secure at all times. You should notify your Local Organisation Administrator (LOA) if you become aware of any unauthorised access to your NHSmail account. You should never input your NHSmail password into any other website other than www.nhs.net. You will never be asked for your NHSmail password. E.g. by phone or email. Do not divulge this information to anyone, even if asked.

3.1.6. Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus software although occasionally, as with any email service, a new virus may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform your local IT services. You must not introduce or forward any virus or any other computer programme that may cause damage to NHS computers or systems. If you are found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service, HSCIC may seek financial reparation from your employing organisation

3.1.7. You must not use the NHSmail service to disable or overload any computer system or network. Where excessive account activity is detected your account could be suspended without notice to safeguard the service for all other users

3.1.8. communication you send through the NHSmail service is assumed to be official correspondence from you acting in your official capacity on behalf of your Organisation. Should you need to, by exception, send communication of a personal nature you must clearly state that your message is a personal message and not sent in your official capacity

3.1.9. You must familiarise yourself with the NHSmail Training and Guidance pages which include important policy guidelines, information about known issues with the service and user/administration guides

3.1.10. If you are accessing your NHSmail account from a non-NHS device (i.e. a home computer, personally owned laptop or in an internet cafe) you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook unless you have explicit permission from your own organisation to do so

3.2. Responsibilities when using the NHSmail email service:

3.2.1. You must not attempt to disguise your identity or your sending address

3.2.2. You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic. If you need to transmit sexually explicit material for a valid clinical reason then you must obtain permission from your local Caldicott Guardian. [Note: GPs may need to refer to the Caldicott Guardian at their local PCT]

3.2.3. You must not use the NHSmail service to harass other users or groups by sending persistent emails to individuals or distribution lists

3.2.4. You must not forward chain emails or other frivolous material to individuals or distribution lists

3.2.5. is your responsibility to check that you are sending email to the correct recipient, as there may be more than one person with the same name using the service. Always check that you have the correct email address for the person you wish to send to - this can be done by checking their entry in the NHS Directory

3.2.6. Email is admissible as evidence in a court of law and messages can be classified as legal documents. Internal emails may also need to be disclosed under the Freedom of Information Act 2000 and the Data Protection Act 1988. Emails should be treated like any other clinical communication and care should be taken to ensure that content is accurate and the tone is appropriate

3.2.7. of the NHSmail SMS/Fax feature is for NHS business use only to support the delivery of Health and social care.

3.3. Responsibilities when using the NHS Directory service:

3.3.1. is your responsibility to make sure that your details in the NHS Directory are correct and up to date

3.3.2. You must not use the NHS Directory to identify individuals or groups of individuals to target for commercial gain, either on your behalf or on that of a third party

3.4. Information governance issues

3.4.1. The General Medical Council (GMC) Good Medical Practice guidance requires doctors to keep clear, accurate and legible records. It is important that emails do not hinder this. You should ensure that relevant data contained in emails is immediately attached to the patient record. Failure to do so could have implications on patient safety

3.4.2. HSmail supports the secure exchange of information and is not designed as a document management system. Documents or emails that are required for retention/compliance purposes should be stored within your organisation's document management system in accordance with local Information Governance policies

3.4.3 Your Organisation is entitled to seek access to the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes without your prior consent. Such requests are strictly regulated with the process detailed in the training and guidance pages

4. Using NHSmail to exchange sensitive information

4.1. The NHSmail service is a secure service, this means that NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail and:

- NHSmail addresses (i.e. from an ‘*.nhs.net' account to an ‘*.nhs.net' account),
- Government secure email domains (between *.nhs.net and *.gsi.gov.uk, *.gse.gov.uk and *.gsx.gov.uk),

- Police National Network/Criminal Justice Services secure email domains (between *.nhs.net and *.pnn.police.uk, *.scn.gov.uk, *.cjsm.net),
- Ministry of Defence secure email domains (*.nhs.net and *.mod.uk),
- Local Government/Social Services secure email domains (*.nhs.net and *.gcsx.gov.uk).

If you intend to use the service to exchange sensitive information you should adhere to the following guidelines:

4.1.1. You should make sure that any exchange of sensitive information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated

4.1.2. ott and local Information Governance principles should apply whenever sensitive information is exchanged

4.1.3. with printed information, care should be taken that sensitive or personal information is not left anywhere that it can be accessed by other people, e.g. on a public computer without password protection

4.1.4. When you are sending sensitive information you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time-sensitive information such as referrals

4.1.5. You must not hold sensitive or personal data in your calendar if your calendar may be accessed by other people who are not involved in the care of that person

4.1.6. If personal identifiable information is visible to other people it is your responsibility to make sure that those people have a valid relationship with the person

4.1.7. You must always be sure that you have the correct contact details for the person (or group) that you are sending the information to. This is especially important if you are sending information using the fax or SMS services. If in doubt you should check the contact details in the NHS Directory

4.1.8. You may only use the NHSmail service for patient referrals if Choose and Book has not yet been implemented in your organisation; the Choose and Book service is unavailable to you for some reason, or the service you need to refer to is not available via Choose and Book

4.1.9. If it is likely that you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen

4.1.10. If using SMS as an alerting or notification system you should ensure you have carried out a relevant risk assessment in relation to the limitation of SMS, particularly its insecure nature and lack of delivery guarantee and delivery notifications. It is not recommended for use where personal data is exchanged or guaranteed delivery is required

4.1.11. Remember that personal information is accessible to the data subject i.e. the patient, under Data Protection legislation.

Appendix 2

Procedures for Mobile Devices and NHSmail

Introduction

NHSmail provides features for mobile users such as wireless synchronisation of the calendar and 'always on email'. Please note should you wish to use a personal device with NHSmail or a mobile device that does not have built-in encryption; please ensure compliance with Trust information governance policies.

NHSmail can only be used on mobile devices with encryption. These include android, windows and apple phone devices.

This document provides guidance on setting up access to a users account from a number of Mobile Devices (mobile phones or handsets that can be used to make phone calls as well as connect to NHSmail).

Key Features of Mobile Devices & NHSmail

- You will receive any new or updated item as soon as it arrives on the NHSmail server – no need to set up a synchronisation schedule
- Email, calendar items, contacts, or tasks can be synchronised 'over the air' with the device – no need to synchronise the calendar or contacts on your mobile with your PC
- Security features are automatically applied to devices that are able to support security policies such as an automatic screen lock after the device has been inactive for 20 minutes, self-service device password reset and remote wipe facility if the handset is lost or stolen. Devices that do not support device policies should only be used in compliance with Trust information governance policies.
- The service is available on different devices including Windows Mobile, Nokia, Blackberry and Apple iPhone 3GS / 4
- Over-the-air search hunts through your entire mailbox on the server and delivers the contents to your device without the need to synchronise it
- Supports flags enables you to manage your email and flag items for later action
- Rich HTML mail for mobile devices renders tables, fonts, formatting and images on the mobile device. You can control whether you want to view HTML or plan text e-mail
- Many bandwidth saving features help reduce airtime costs and the time taken to deliver data over slow wireless networks
- You can forward, reply, or reply all to a meeting request
- If you forget to set your out of office message you can do so on your mobile device
- Ease of setup with Outlook's 'Autodiscover' – all you need to know is your email address and password.

How to Set Up Your Mobile Device to Access NHSmail

- To ensure all NHSmail users benefit from the performance, functionality and security features of the service on a mobile device, it is not possible to connect mobile devices using the IMAP/POP method

- The service uses an encrypted link between the device and the NHSmail service providing for the secure exchange of email between NHSmail recipients.

Configuration guides for the following mobile devices can be found in the 'Mobile devices, applications and email programmes' section of the NHSmail Training and Guidance pages:

- Apple iPhone
- Windows Mobile
- Apple iPad
- Android devices

For assistance with setting up your mobile device please contact the IT Service desk (x85777).

Important note: some mobile devices provide an initial synchronisation option of replacing the Calendar and Contact information in your NHSmail account with the data held on the device. If you select this option all existing calendar and contact information in your NHSmail account will be removed and replaced with the data on your device and it could, as a result, be left blank.

If you erroneously select this option there is no way to recover your NHSmail Calendar and Contacts unless you have your own personal backup. This is because although it is possible to recover deleted items in NHSmail up to 14 days after the event, your handset has instructed the service to change, not delete, the data in your account.

Information for Current Mobile Device Users:
Once the new mobile security policy is switched on in December 2010, any mobile devices will be blocked from accessing NHSmail if it is not one of the devices that fully enforce the security features and have a suitable built-in capability to encrypt the data held on it. Any previously synchronised data will remain on the device but should be removed for security reasons.

How to Protect Data if Your Mobile is Lost or Stolen

If you lose your mobile device or it is stolen it's important that you wipe the data it contains in order to keep any sensitive information safe. You can do this from your NHSmail account by following the steps below:

- Log into NHSmail via the NHSmail web browser and disable device
- From your inbox click on 'Options' in the top right
- Click on 'Mobile Devices' in the left hand menu
- Click on 'Wipe all Data from Device'

The national NHSmail helpdesk can also do this for you but the request must come from your Local Organisation Administrator.

Pro's and Con's for accessing email via mobile device.

Pro's

- Most devices (including Trust owned and Personal devices) can be setup to access NHS Mail
- Once setup email is then available from any location with a data\wireless connection
- Enables the ability to read and respond promptly to email
- There is no requirement for laptops and tokens to access email

Con's

- Increase in Trust mobile data costs as more people download emails
- Always connected, therefore feel the need to respond to emails promptly and out of hours

Appendix 3

Sharing Sensitive and Patient Identifiable Data (PID) via Email

Below is a summary of the secure way of transmitting such information:

- NHSmail to NHSmail is encrypted and therefore secure
- Encrypted attachments are blocked and will be removed by NHSmail and a number of government email systems, to avoid the risk of computer viruses being sent or received. Should an encrypted attachment bypass NHSmail security, automatic detection updates will remove the attachment of any historic item
- NHSmail to certain central and local government domains is secure:
    - Central Government
        - *.gsi.gov.uk
        - *gse.gov.uk
        - *.gsx.gov.uk
    - Ministry of Defence
        - *.mod.uk
    - Police National Network/Criminal Justice Services
        - *.pnn.police.uk
        - *.scn.gov.uk
        - *.cjsm.net
    - Local Government/Social Services
        - *gcsx.gov.uk
- Regular information flows from NHSmail users to non-secure domains should be facilitated via the NHSmail third party programme (https://web.nhs.net/public/InformationGuidanceServices/DefaultPage.aspx)
- One-off messages from NHSmail users to non-secure domains should be sent using the S/MIME encryption tool via Outlook
- The transmission of patient identifiable information to or from a local NHS email system (*.nhs.uk) is not secure. As the transmission can involve messages being routed over the internet, encryption solutions are required.

Appendix 4

NHS Blocked Email Attachments

To prevent inappropriate material being sent by NHSmail there are a number of attachments that will be blocked from the service.

The following file types are blocked on the Relay and NHSmail services.

File Type	Description
Avi	Audio Video Interleaved animation file
Bas	BASIC programming files
Bat	DOS batch file
Chm	MS compiled HTML help file
Cmd	OS/2 or Windows NT batch file
Cnt	Helpfile contents
Com	16-bit DOS executable
Cpl	Windows Control Panel extension
Crt	Security Certificate
Eml	Outlook Express mail message
Exe	DOS or Windows 16/32 bit executable Please note: there is an issue when attempting to send exe attachments via the NHSmail portal. Mail should be delivered with the .exe file stripped out and replaced with a message explaining that the file has been removed. Instead the sender is presented with an error message and the mail isn't delivered.
Hlp	Windows help files: 16-bit executable
Hta	HTML file
Inf	Windows help files: 16-bit executable
Ins	Internet naming service
Isp	Internet communication settings
Js	JavaScript file
Jse	JavaScript encoded script
Lnk	Windows shortcut file
Mpe	MPEG Movie Clip
Mpeg	MPEG Movie Clip
Mpg	MPEG animation
Mp2	MPEG audio file
Mp3	Mp3PRO Audio file
Msc	MS common console doc
Msi	Windows installer file
Msp	Windows installer patch
Mst	Visual test source file
Pcd	Photo CD image
Pif	Program Information File
Reg	Windows registry file
Scr	Screen saver
Sct	Windows script component
Shs	Windows scrap object
Vbe	Visual Basic encoded script
Vbs	Visual Basic script
Wsc	Windows script file
Wsf	Windows script file
Wsh	Windows scripting host settings file

Appendix 5

Procedure for Generic Email / Generic Password Control

The purpose of this Procedure is to identify the criteria under which it is permissible to establish generic email accounts (rather than providing proxy access) and likewise under what circumstances it is permissible to use generic passwords, rather then issuing each unique user with their own unique user id, in accordance with Trust IT Security and Information Governance policies.

Aim and Scope

There is currently no national guidance available within the NHS with regard to the use of generic email and/or generic password controls. These procedures are intended to provide workaround solutions that address these two important issues.

Numerous generic email addresses are already in use within the Trust e.g. dhft.Communications@nhs.net and dhft.DerbyHospitals@nhs.net. There are clear benefits to the use of such accounts in certain circumstances, but it would be unwise to agree every request without careful thought and consideration. These procedures set out to control the establishment and ongoing usage of such accounts.

Similarly, there are certain circumstances whereby it is not possible to utilise individually attributable logon accounts and passwords, e.g. where a computer needs network access in order to let users into a clinical system, but where the clinical system does require a unique user ID. These procedures seek to control use of generic accounts to circumstances where the clinical benefits clearly outweigh the risks involved in operating such a system.

Generic Email

Requests for Generic email accounts must be made via the IT Service desk.

They will be considered by the Information and Records Governance Co-ordinator in accordance with the following criteria:

- Access required by secretary/personal assistant for the purpose of managing emails/diary appointments etc…**proxy access should be granted. Note:** When replying on behalf of another individual, emails must be concluded with the name of the person actually sending the correspondence. This is in keeping with the way in which secretaries traditionally signed correspondence as **"pp"**.
- Patient or staff led service would be made significantly easier to operate if patients or members of staff could be given one central email address, rather than a number of named individual…**generic email address should be granted. Note:** Departments will need to have robust procedures in place to ensure the generic mailbox is checked and actioned on a regular basis.
- Where requests are made to set up generic email addresses for the purpose of allowing patients to contact the hospital to change appointments, these will only be allowed in circumstances where the department can prove that patients are warned of the risks involved and documented consent is received from patients concerned indicating they are prepared to accept the risk and any incidents which may occur as a

result of their information being intercepted. Such consent must be recorded in the patient records.

A log of generic email addresses will be maintained on the Information Governance drive.

General User ID/Password Combinations

Requests for Generic User ID/Password combinations must be made through the IT Service desk.

They will be considered by the IT Service desk/Information Governance Team in accordance with the following criteria:

- Workstation needs to remain logged in to network throughout the day to facilitate individual members of staff gaining speedy access to clinical systems using their own individual log on (e.g. workstations in A&E)…**generic username should be set up with read only access to application areas only (i.e. no access to areas of server where data files are stored).**
- Clinical system needs to connect to another clinical system through interface engine or the like…**generic username should be set up. Use should be audited on a regular basis to identify any suspicious usage. Note:** Obvious user names (e.g. Supervisor, Admin) should be avoided.

A log of generic user accounts will be maintained on the Information Governance drive.

Application for Generic Email Account

Derby Hospitals NHS
NHS Foundation Trust

Helpdesk Reference Number:

Name of person requesting the email:

Date requested:

Date requested:

1) Please provide names of all those requiring access.

Name	Name
e.g. Joe Bloggs	

2)Why is the generic mailbox needed? (please give as much detail as possible)

3)What information will be sent and received from the account? Please provide details below:

a) **Will this include patient/staff demographics (name, address, dob etc)?**
b) **Will the information be clinical/sensitive information (medical history, diagnosis etc)?**
c) **How many patient/staff details will be sent in any one email?**

4)How is the information being currently sent? If it's via email please state the addresses the information is sent between.

5)If the mailbox is to be used for clinical communications i.e. sending information to a patient please indicate:

a) **What steps will be taken to ensure that patients are warned of the risks involved in receiving such communications by email?**
b) **How and where will patient consent be recorded?**
c) **Has this communication with patients been approved?**

(Please note: consent must include a signed declaration from the patient to the effect that they are prepared to accept the risk and any incidents that may occur as a result of information being intercepted).

What is the preferred address for your generic mailbox:

Please can you return to the Information Governance Team at dhft.informationgovernance@nhs.net

Office Use Only
Has the Caldicott Guardian approved the use of the email address?

Caldicott Guardians Comments

Appendix 6

Procedure for Using NHSmail for Clinical Communication

Introduction

NHSmail is a secure service approved for the exchange of patient data between NHSmail recipients.

The NHSmail service provides encryption of interpersonal messages during transmission. This ensures that the message cannot be intercepted and read or tampered with during transmission. The service currently does not address the issue of authentication. The provision of digital signatures for certain categories or users is scheduled for a future release of the programme. This Procedure is to ensure that clinical information is protected until authentication is in place.

However, although NHSmail is a secure messenger service, it does not protect information before or after it has been received. If used for clinical communications then, as with current paper systems, it must be ensured that once delivered, the information will be properly protected and acted upon, in accordance with local Information Governance guidelines.

Acceptable Use of the Account

Derby Hospitals NHS Foundation Trust (DHFT) will create and manage a generic NHSmail email account for clinical communications requests. This will be called dhft.****@nhs.net

The non-DHFT NHS organisation will create a generic NHSmail email account for the clinical communications request. Once created, the ownership and management of the account will rest with the relevant non-DHFT NHS organisation.

Only authorised staff will have access to the mailboxes.

Once received, the information must be handled in accordance with local Information Governance policies and guidelines.

The generic NHSmail accounts must only be used for a specified purpose and all staff must be trained and made aware of the sensitive nature of the information being transmitted. Only the agreed process as outlined in the workflow must be used.

When creating an email, the address must be selected from the NHSmail address book to ensure the correct format and spelling (where practical this should be saved into the 'Contacts' of the 'clinical communications' email account for ease of selection). The address books will be maintained by the DHFT and non-DHFT NHS organisation mailbox owners.

Access Rights

No staff will have access to the shared account unless they have already registered on NHSmail.

The DHFT and non-DHFT NHS organisation mailbox owners will maintain a list of staff who have access to each mailbox. Staff no longer requiring access must be deleted immediately.

Workflow for 'Sending Clinical Communications' Account

The 'Sending' and 'Receiving' organisation has a generic NHSmail 'clinical communications' account (accessed via users personal email account), from which clinical communications emails must be sent and received. Clinical communications emails should not be sent or received by the user's individual NHSmail account.

The email must have an agreed format for the subject title. The body of the email must be standardised, and where practical pre-populated.

Delivery receipts and Read receipts must be set up to confirm that the clinical communication has been received, read and is being processed.

INFORMATION GOVERNANCE PRINCIPLES MUST BE APPLIED FOR THE SAFE USE AND HANDLING OF PATIENT DATA.

Workflow for 'Receiving Clinical Communications' Account

The 'receiving clinical communications' mailboxes will be checked as specified in the agreed procedure. On receipt of a clinical communication, the email will be opened and processed in accordance with the agreed procedure.

The 'Receiving' account will automatically send a read acknowledgement when the email is opened (where a read receipt has been requested).

Hardware and Browser Settings

The browser must support 128bit SSL encryption and the advanced options must be enabled to "empty temporary internet folder when browser is closed".

Ownership and Responsibility

The Manager of the appropriate section within DHFT will be responsible for the correct use of the accounts accessed by DHFT staff.

The Manager of the appropriate section of the non-DHFT NHS organisation will be responsible for the correct use of their 'clinical communications' NHSmail account, which is accessed by staff within their NHS organisation.

Good Email Practice **Appendix 7**

The Trust email is a means of business communication. Emails are disclosable in law and under the Freedom of Information Act.

Subject headings for emails

- Subjects should be relevant, clear and brief, this will help file, retrieve and prioritise the content of the message. Do not include the name of an individual (patient or staff).

Content of emails

- Type the message using conventional punctuation, with upper and lower cases (using all capitals is considered aggressive).
- Keep it short and simple – avoid sending lengthy emails.
- Be careful about the content – do not write something that you would not write in a letter or say face to face with someone. Remember that an email is not a substitute for a telephone call.
- Put different topics in separate emails; don't put them in one long email.
- Always sign off with your name, job title and telephone number. The system has the facility to set up an electronic 'signature' if you are not sure how this is done then contact the IT Service desk on Ext 5777 for assistance.

Sending emails

- Use the 'To' and 'CC' options appropriately. If you put an address in 'To' – you want the person/staff group to **action** any requests in your email.
  'CC' is used to for the addressee's **information only** and they are not expected to act upon receiving your email.
- The autofill function will predict the name of the recipient however, care must be taken as there may be several entries in address book with the same name.
- Be selective about who receives your email, especially when you using the 'reply to all' option. Ask yourself do all recipients need to see your reply?
- Do not enter in a perpetual loop of 'Thanking' people for their email as this causes unnecessary traffic on the network.
- Avoid sending large attachments to large numbers of staff as this can drastically affect the network. If applicable reference the server and file path that they can be found on.
- Where possible include a link rather than an attachment.
- Always check your email before sending it. Ensure that attachments are complete and correct.
- If you need an answer say so in your message and always follow up.

Saving emails.

- Copy into a network server structure

Mailbox

It is imperative that your received emails are regularly reviewed and deleted if no longer relevant

Inappropriate emails

If you receive any emails that you consider to be unnecessary delete them and inform the sender that you do not wish such information again.

Unknown Sources and Work Related only

Email should only be used for work related matters. Do not open any emails from sources unknown to you as they may contain viruses. Check with the ithelpdesk and delete.

Housekeeping

It is essential that your email area is kept up to date. There are 3 automatic functions.

- Trash should be set to auto delete after 30 days as a maximum.
- Mail and phone – set to own personal setting
- Appointments, tasks and reminders – set to own personal setting

The following areas will need to be manually cleared:

- Filing – folder contents
- Sent Items

It is essential that the system is effectively maintained in order to ensure that it operates to its full potential. Poor management will have an adverse effect on the responsiveness of the system and storage capacity.