



Email Acceptable Use Policy 2011-2013

Approval Process

Lead Author: Anglia Support Partnership (ASP)

Reviewed /
Developed by: Information Governance Steering Group Members

Approved by: Information Governance Steering Group

Ratified by: Governance and Compliance Committee

Date ratified: September 2011

Version: 1

Latest revision
date: none

Review date: September 2013
(or earlier if significant change to local or national
requirements)

Valid on: September 2011

Signatures for Ratification

1. Name	Title
Signature	Date
2. Name	Title
Signature	Date

Document Control Sheet

Development and Consultation:	Policy developed in consultation with Information Security Manager (ASP), Information Governance Team (NHS Cambridgeshire), Information Governance Steering Group (NHS Cambridgeshire) and endorsed by the Healthcare Governance Committee and PCT Board.
Dissemination	This policy will be promoted within NHS Cambridgeshire (the Commissioning PCT) and uploaded to the website
Implementation	The Information Governance Steering Group is responsible for monitoring the application of the policy by ensuring that: - <ul style="list-style-type: none"> • The policy is brought to the attention of all employees • Managers are aware of their responsibilities for ensuring that staff under their control implement the policy • Appropriate training and guidance is provided to staff • Corporate business processes support the implementation of the policy
Training	Training will be undertaken as part of the PCT's ongoing processes.
Audit	Implementation of the Policy will be monitored on a regular basis. ASP will carry out reporting and monitoring on behalf of the PCT.
Review	This policy will be reviewed bi-annually, or earlier if there are changes in procedures or legislation.
Standards for Better Health	This policy supports the PCT in its compliance with the Information Governance Toolkit and legal compliance with Data Protection Act, Misuse of Computers Act 1990, Privacy and Electronic Communications (EC Directive) Regulations 2003 and NHS Code of Confidentiality.
Links with other DtGP	The Policy should be read in conjunction with the following other policies which can be found on the NHS Cambridgeshire website (www.cambridgeshirepct.nhs.uk) : <ul style="list-style-type: none"> Code of Conduct for Confidentiality Data Storage Best Practice Policy Disciplinary Policy Home working Policy Incident and Near Miss Reporting Guidance Information Governance Policy Information Sharing Protocol Internet Acceptable Use Policy Information Security Staff Policy NHS Cambridgeshire Code of Confidentiality Removable Media Policy Safe Haven Policy Home Working Policy Records Management Policy
Equality and Diversity	The Information Governance team have carried out a Rapid Equality & Diversity Impact assessment and concluded the policy is compliant with the PCT Equality and Diversity Policy. A few negative impacts were identified and Action Plan identifies these.

Table of Contents

	Page
1. Introduction.....	4
2. Purpose and scope.....	4
3. Roles & responsibilities.....	4
4. Dissemination and implementation.....	5
5. Prohibited use.....	5
6. Best practice	5
6.1 Rules for email.....	5
6.2 Closing email accounts	7
6.3 Access to another individual's mailbox.....	8
6.4 Automated forwarding of email.....	8
6.5 Email and home working.....	10
6.6 Auto-signature and disclaimer.....	10
6.7 Out of Office assistant.....	11
6.8 Housekeeping and archiving.....	11
7. Email security & information governance.....	11
7.1 General rules for confidential and sensitive email.....	11
7.2 Use of nhs.net.....	12
7.3 Sharing confidential information.....	13
7.4 SPAM & phishing email.....	14
7.5 Attachments.....	14
8. Acceptable personal use.....	15
8.1 Examples of acceptable personal use.....	15
8.2 Criteria for determining acceptable use.....	15
9. Non-compliance.....	16
10. Monitoring.....	16
11. Emailing patients/service users.....	17
Appendix 1 Emailing Patients – Trust Request Form	
Appendix 2 Glossary of Terms	
Appendix 3 Email Security Tiers	

1. Introduction

This Email Acceptable Use Policy (EAUP) outlines the permissible use of business email for NHS Cambridgeshire when accessing services from the workplace or using NHS resources remotely (e.g. laptop connected to VPN at home)

This policy applies to all employees of NHS Cambridgeshire including contracted and temporary staff.

Staff are advised to familiarise themselves fully with this policy and to have due regard for professional behaviour and etiquette when carrying out any type of communication on behalf of the organisation.

2. Purpose and scope

NHS Cambridgeshire recognises that email is a useful means of communication, a valuable resource and essential to support NHS business. Email enables employees to communicate promptly and efficiently with other employees, individuals and organisations and for them to undertake their role efficiently and effectively.

The purpose of this policy is to ensure the proper use of email, so all employees are aware of what is deemed as acceptable, and unacceptable.

Email is primarily for business use. Employees are permitted to use email for occasional and reasonable personal use, subject to the terms in this policy. Email carries the same legal status as other written documents and should be treated with the same care

Occasional and reasonable personal use of email is a privilege and not an entitlement. This privilege may be withdrawn at anytime, for either a specific individual or for all employees of the organisation. Employees will be informed prior to access being revoked.

3. Roles & responsibilities

All staff in the organisation are responsible for ensuring the safe receipt, maintaining and disclosure of person identifiable information is done in line with this policy and that good practice is maintained throughout the organisation. Failure to comply with this policy may result in disciplinary action being taken.

The Caldicott Guardian is responsible for ensuring person identifiable clinical information is received, stored and used in line with the Trust obligations to the Data Protection Act 1998 and the NHS Connecting for Health, Information Governance Toolkit.

Senior Information Risk Owner (SIRO) is responsible for leading and fostering a corporate culture which values, protects and uses information for the success of the organisation and benefit of its customers.

Directors and Managers are responsible for ensuring Trust Email procedures are known and followed in their areas.

Administrative Staff are responsible for following Trust policy and contributing to good practice within the Trust.

Clinical Staff are responsible for ensuring information is dealt with appropriately and professionally both in line with this policy and to their professional code of conduct.

4. Dissemination and implementation

The responsibility for disseminating and implementation of this policy lies with the local Directors and Managers.

The policy will be implemented immediately on receipt. See Document Control sheet.

5. Prohibited use

The following list is not exhaustive, but provided as an indication of prohibited use of email, including creating, sending and forwarding email messages which pertain to any of the following contents or activities:

- Any pornographic, obscene, indecent or sexually explicit material
- Any illegal material
- Any offensive, harassing, sexist, racist, hateful or otherwise offensive/discriminatory material
- Chain messages and jokes
- For any private commercial activities (e.g. running a business)
- To perpetrate any form of fraud or criminal activity
- Any form of defamation, discrimination, harassment or bullying
- For the introduction of viruses, spyware or malware
- 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
- For illicitly distributing any person identifiable or business confidential material
- For abusing the use of email, e.g. using email like instant messenger
- Sending personal emails to large number of recipients e.g. concert tickets for sale
- Subscribing to forums using your work email address
- Representing personal opinions as that of the organisation
- 'Spamming' or sending bulk unsolicited emails
- The automated forwarding of NHS emails to public Internet email addresses
- For personal financial gain
- Infringement of copyrights
- To represent yourself as someone else

6.

6.1 Rules for email

6.2 Closing email accounts

For access security purposes it is important to ensure the email account(s) for a member of staff is (are) closed once they leave employment. The Line Manager is responsible for ensuring an email account is closed by completing the NHSC3 – ICTS Systems Access – Leavers Only form and sending to ASP. Forms sent electronically should be sent from a Director or Assistant Director's mailbox.

6.3 Access to another individual's mailbox

For planned absence, software delegation tools should be used as appropriate to grant someone else 'read' permissions to your mailbox (*Go to Outlook / Tools / Options / Delegates*). We recommend staff arrange pre-authorized access in advance of any emergency.

For access to another user's mailbox in unexpected circumstances - such as sick leave and personal emergencies where absence from work is unexpected - where there is an immediate business need to have access to this information; the following steps need to be followed:

- Email authorisation from the employee's Director to the ASP IT Service Desk is required. This should name the person requiring access, and the expected duration.
- Based on business need, the email from the Director should state if access to the Inbox is required, or the entire Mailbox, including Sent Items and sub folders.
- The employee should be informed of the access, business justification, the nominated individual who had access, and the period of time.
- Any emails marked as 'Private' or 'Personal' in the subject heading must not be read, as the purpose of the above is to access business information.

6.4 Forwarding of emails

Staff must not forward work emails from their PCT account to a personal / home email account.

6.41 Automated Forwarding

It is recognised that on occasions it may be necessary to automatically forward email from one account to another. However before undertaking automated email forwarding, please consider the following points:

- Why do you need to automatically forward email? Can you gain remote access to the original mailbox? Could you leave an Out of Office message stating to contact you on an alternative email address or by phone? Do you need multiple email addresses? Could you use nhs.net, which can give you access from all sites?
- The automated forwarding of emails to public Internet email addresses (e.g. hotmail, yahoo) is strictly prohibited.

- If incorrectly configured, automated email forwarding can create a 'loop' which will generate tens of thousands (or even hundreds of thousands) of email messages and fill up quotas.
- You should not automatically forward from one colleague to another – use the Delegates option to allow a colleague to gain access to your Inbox e.g. for the period of time you are away.
- If you apply automated email forwarding you may be asked to justify why you did this, and what alternative options you considered.
- Automated forwarding of email has to be initiated by the member of staff who owns the Inbox. The ASP IT Service Desk and ASP IT Engineers will not undertake automatic forwarding on your behalf. You remain responsible for the automated email forwarding at all times.
- Staff can only auto-forward emails from nhs.uk to nhs.net if this does not include confidential and sensitive data. You cannot auto-forward email from nhs.net to nhs.uk as the system does not allow this functionality.
- If you are in any doubt, please contact the ASP IT Service Desk on 0800 996 996 or email aspitservicedesk@asp.nhs.uk

6.5 Email and home working

When working at home staff should use a Trust laptop and Trust VPN token to access the PCT's secure network.

Staff are permitted to use their home computer for use of their nhs.net email account only, but not to download from nhs.net. Staff are otherwise not permitted to use home computers until the Trust provides an IT remote home working solution. The Home Working Policy assessment should be completed by all staff who routinely work at home

6.6 Auto-signature and disclaimer

The use of email disclaimers are recognised as good practice, though not legally binding. The following format should be used in Arial, 10pt, black type:

Name
 Job Title
 Tel: 01223 123456
 Fax: 01223 123456
 Mobile: if you have a work mobile number
 Email: name.surname@cambridgeshire.nhs.uk
 Secure Email: name.surname@nhs.net
 Website: www.cambridgeshire.nhs.uk
 SPACE
 NHS Cambridgeshire, Address.

This message may contain confidential and privileged information. If you are not the intended recipient please accept our apologies. Please do not disclose copy or distribute information in this email or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful.

Please inform us that this message has gone astray before deleting it. Thank you for your co-operation.

6.7 Out of Office assistant

If you are going to be out of the office for more than one day, you should turn on your 'Out Of Office' (*Go to, Tools / Out of Office Assistant*). When this is turned on it will automatically reply with a given message to anybody that sends you an email. The 'Out Of Office' message should state when you will be able to reply to the message and alternative contact details for colleagues that may be able to assist. Colleagues listed in an out of office assistant message should be made aware of this prior to this being enabled.

6.8 Housekeeping and archiving

Email capacity is not unlimited. Staff should regularly delete unwanted emails from their Inbox (including sub folders) and Sent Items. Once this is done, staff should remember to empty their Deleted Items folder.

If you receive an email from the 'System Administrator' you will need to start to delete unnecessary email. Please note it is the size of the email (usually due to attachments) and not number of emails that will fill up the quota. If you genuinely need to keep old emails for business reasons, then you can move these to an Outlook Personal Folder. If you need assistance in setting up a Personal Folder please contact the ASP I T Service Desk.

7. Confidential and sensitive emails

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored and can include: patient data; professional and contract performance data; information around HR, payroll, salaries and occupational health; sensitive requests, complaints, investigations, papers for meeting that contain confidential subject matter, Serious Case Reviews, and Serious Untoward Incidents. See Glossary of Terms, Appendix 2.

All employees are responsible for maintaining the confidentiality of information and complying with the Caldicott Principles and Data Protection Act.

Breaches of confidentiality must be reported to the IG team, the Risk Coordinator and Information Governance Champion.

Emails containing person identifiable or sensitive information must be stored appropriately on receipt, e.g. incorporated within the health record, and deleted from the email system when no longer needed

7.1 Use of nhs.net email (also known as NHSmail)

- If the subject chooses to email their own sensitive information to your PCT email account rather than your nhs.net account, this is their choice and is acceptable so long as it is NOT sent on behalf of an NHS organisation as

they should set up an nhs.net account for this. PCT staff should still reply via nhs.net. See the section 'Emailing Patients' and Appendix 1.

- When sending an email to a network distribution list, you should check the distribution list membership prior to sending the email to ensure that the membership is appropriate.
- Take particular care when forwarding emails to ensure that you do not cause damage, embarrassment or disclose confidential material to the originators and other recipients of the email.
- Take particular care with the use of the 'Reply to All' function in email, considering that many (sometimes hundreds) of recipients may receive your response.
- Never use a person's name as the subject heading of an email

NHSmail must be used by NHS staff when sharing person / patient identifiable or business sensitive information via email.

NHSmail is the brand name for nhs.net email. Nhs.net is a secure national email service which enables secure exchange of sensitive and patient identifiable information within the NHS and with local / central government. All user connections to the service are encrypted, this removes the need to encrypt or password protect attachments.

Nhs.net is the only BMA and Department of Health approved email service for the secure exchange of clinical data between NHS organisations and the government email domains below:

Central Gov	x.gsi.gov.uk	.gsi.gov.uk	.gse.gov.uk
	.gsx.gov.uk	.police.uk	.pnn.police.uk
	.cjsm.net	.scn.gov.uk	.mod.uk

Local Gov	.gcsx.gov.uk
-----------	---------------------

- Email addresses given out to the public, or NHS professionals, on publicity material or on websites as part of formal public engagement work (e.g. audit, complaints, research) should be nhs.net addresses not PCT email addresses and any webpage for such work should recommend NHS colleagues correspond via nhs.net.
- *Only* nhs.net should be used by NHS staff when sharing person / patient identifiable or business sensitive information via email. The recipient's email address must be either nhs.net or one of the listed secure government domains.
- Nhs.net accounts should be set up as name.surname@nhs.net , and name.surname2@nhs.net etc where there is an existing account with your name.

- Encrypted attachments are blocked by the nhs.net service and a number of government email systems, to avoid the risk of computer viruses being sent or received. Any attempts to bypass encrypted security controls in nhs.net must be avoided.
- Staff are permitted to use their home computer for use of their nhs.net email account only, but not to download from nhs.net. Staff are otherwise not permitted to use home machines until the Trust provides an IT remote home working solution.

7.3 Sharing confidential information by email outside of nhs.net and government domains

Email to third parties will be dealt with on a case by case basis. Nhs.net users that need to share confidential information with individuals who do not have nhs.net email or a secure government email should speak with a member of the Information Governance team (NHS Cambridgeshire) in the first instance.

Do

- Advise external NHS colleagues to send person / patient identifiable information and business sensitive information to your nhs.net email.
- Check both email account - nhs.net account and PCT - as it is the email account holder's responsibility to check.
- Include your nhs.net address on your PCT email signature.
- Seek information governance advice before sending sensitive emails to a non-nhs.net / non-government domain account.
- Make sure the nhs.net address on any publicity literature or webpage is spelled correctly.
- Report Serious Incidents (SIs) via an nhs.net account

Don't

- Forward emails from an nhs.net to an unsecure email account.
- Configure an nhs.net account to 'Outlook' on either a home or work computer.
- Guess the nhs.net address for an individual. Check you have the right address either by phoning and asking the individual or by using the nhs.net directory to check an individual's name with other details e.g. their organisation, to ensure the correct email address is being used. It is the account holder's responsibility to keep their details updated.

7.4 SPAM & phishing email

SPAM email is unsolicited email, often referred to as 'junk' email and is indiscriminately sent to many thousands (if not hundreds of thousands) of email addresses. SPAM email usually invites you to purchase a product or service.

Phishing (pronounced Fishing) is an attempt to fraudulently acquire sensitive or person identifiable information like credit card details, bank account details, passwords or other similar information, usually by masquerading as a trustworthy source e.g. your Bank. Phishing is typically carried out by email with a link to a website, and often asks you to enter your personal details e.g. bank accounts details, password etc into a website. (Never respond to such a request to divulge your personal information).

SPAM/Phishing email is filtered in two ways:

- 1) Emails guaranteed to be SPAM/Phishing will not be delivered to your inbox.
- 2) Emails suspected to be SPAM will be delivered to your inbox, but marked with [SPAM] in the subject heading. If these emails are SPAM and they are not required they can be deleted.

Any emails that are incorrectly 'tagged' should be forwarded to the 'Anti SPAM/Phishing' mailbox on the Global Address Book.

Never reply to any SPAM or Phishing emails.

7.5 Attachments

The emailing of office attachments including (.doc .ppt .xls etc) is supported across the NHS Cambridgeshire / ASP network.

Sending of .exe files and movie files (unless these are for business purposes) is prohibited.

You can avoid cluttering up Inboxes with unnecessary attachments by referencing the document with a link to a file in the shared drive or to a webpage, rather than attaching the document itself. *[To include a link to a file path in your email staff will need Outlook 2003 or later. Select New Message, click on the paperclip icon, locate the file and select it, click on the drop down arrow beside the Insert button and select Insert as Hyperlink.]* Please note that this solution is only available to individuals who have access rights to the drive and folder or website that the file is stored in.

Great care should be taken when attaching documents or referencing documents, as the ease with which employees can download files from the Internet, or cut and paste materials from electronic sources increases the risks of infringement of the rights of others, particularly the intellectual property and other proprietary rights. Also attaching documents may give rise to breach of confidentiality, hence the importance of vetting attachments. If in doubt, please consult your manager.

See also NHS Cambridgeshire, Data Storage Best Practice Policy.

8. Acceptable personal use

Email is primarily for business use. Employees are permitted to use the email for occasional and reasonable personal use, subject to the terms of this policy. It is a privilege, not an entitlement, which may be withdrawn at anytime for either a specific individual or for all employees of the organisation. Employees will be informed prior to access being revoked.

Personal use of email must be restricted to breaks or occur outside of the employee's normal working hours.

All personal emails should be marked 'private' or 'personal' in the subject heading of the email, all other emails will be considered as business emails and therefore subject to monitoring.

8.1 Examples of unacceptable personal use

The following scenarios have been described as unacceptable personal use of the Internet:

1. A member of staff uses their work email address to apply for new jobs.
2. A member of staff forwards jokes received onto colleagues and external recipients.
3. A member of staff subscribes to forums with their work email address.
4. A member of staff replies to 15 emails throughout the day organising their social life.

8.2 Criteria for determining acceptable Use

When considering acceptable personal use of email you will need to consider:

- Your own work
- The work of colleagues
- The impact to the department's service delivery
- The time of the day, restricted to breaks and/or outside of normal working hours.
- Perception that others will have of you using email for personal use
- Duration that you expect this to take you
- Frequency of personal use of email
- The recipient that you are sending the email to
- The content of the email message
- That the email message will come from your work account and be associated to the organisation.
- That the email shall be marked 'personal' or 'private'.

Broadly the criteria for determining acceptable personal use should be similar to that of employees making telephone calls of a personal nature within business hours, such as making appointments.

9. Non-compliance

Any breach of this policy, including excessive personal use of the email can result in disciplinary action up to and including dismissal, according to the organisation's disciplinary policy. Non-compliance can also damage the reputation of the organisation and open the organisation and individual to a host of legal liabilities.

Access to the email requires system access that must be authorised by your line manager. Sharing passwords, and logging onto the network as another individual is also a disciplinary offence and a breach of this policy, the NHS Cambridgeshire Code of Confidentiality and the Information Security Staff Policy.

10. Monitoring

All employees need to be aware that the employing organisation can monitor the use of email facilities for the following reasons:

- To ensure compliance to this policy.
- To protect the Trust from a host of legal liabilities including harassment and discrimination in the work place, defamation, transmitting of confidential information.
- To guard against inappropriate and excessive personal use.
- Monitor use of broadband connection to maintain business continuity.

If any breach of this policy is observed, disciplinary action will be taken

The provisions of the Data Protection Act 1998 (and any related legislation) and the Freedom of Information Act 2000 and the organisation's policies and procedures relating to Data Protection, Freedom of Information, and confidentiality also apply to email communication. This means that emails may have to be disclosed to individuals or outside agencies, as required by current Data Protection and Freedom of Information legislation or as required by any other statutory or legal duty imposed on the organisation

All personal emails should be marked 'private' or 'personal' in the subject heading. The email should also state that it is being sent in a personal capacity and not representative of the organisation. All other emails will be considered as business emails and therefore subject to monitoring. Although in normal circumstances the content of the personal emails will not be monitored, the number of personal emails will be. However if there is a reasonable belief that the personal emails contain information of the following nature, then a Senior ASP IT manager may review the content of the email:

- Harassment and bullying.
- Defamation of the Trust or an individual employee.
- Transmission of confidential information.
- Any activities, which could be potentially be construed as gross misconduct under the disciplinary policy and as such require full investigation.

If the monitoring highlights potential misuse or abuse, or contains any information of an inappropriate nature the information will be passed to the relevant NHS Cambridgeshire Director. The Director will be responsible for deciding further action in consultation with the Caldicott Guardian and / or Senior Information Risk Owner. In addition to this, if monitoring necessitates the need to refer to external agencies such as Audit or the Police, then the Trust will do so as soon as practically possible.

11. Emailing patients/service users

It is recognised that email can be an efficient communication method between a clinician and a service user. The form in Appendix 1 should be used when emailing patients. The risks associated with emailing patients include, but are not limited to:

- Email to public Internet email addresses (e.g. name@googelmail.com) is not secure at any point.
- An unlocked PC or a publically situated PC could result in a confidential email being left open to view
- The email could be forwarded to another email recipient.
- The email could be sent to the wrong patient, unless an email link is created.
- The email could be printed and passed to other individuals.
- If the patient gives you a work email address, this address will usually name the organisation that the patient works for.
- A virus could spread this personal and sensitive email to other individuals.
- If an attachment is used then a 'cached' copy of this file will reside on the PC that the email is opened on (e.g. the patient/service user), and can be accessed by others who have access to this PC.

Emailing Patients – Trust Request Form

Request for Trust to contact patient via personal email address.

The XXXXXXXXXXXXXXX Trust is committed to open working and efficiency in providing services. To ensure that services are as tailor made as possible to the requirements of its patients the Trust recognises that with advancing technology, current and routine forms of communication may not be convenient or possible with some patients. To this end the Trust will be willing to undertake email correspondence with the patient under the following conditions.

- This agreement is entered into at the request of the patient
- The patient understands that the Trust has no responsibility for information that leaves authorised NHS (National Health Service) networks at the request of the patient and as such cannot guarantee the security of such information
- The patient understands that the Trust has no responsibility for equipment used by the patient to send or receive email
- The patient has satisfied themselves that access to their own system is secure and are aware of shared email accounts, shared computers etc.,
- To minimise the risk of ‘human error’ in writing email addresses, the patient will send an email to XXXXXXXXXXXXXXX in the first instance. This will give the Trust their preferred email contact address and will be used to correspond with them. A test email will be returned by the Trust to indicate safe receipt and that the sent address will be the one used to correspond with the patient.
- The Trust reserves the right to terminate this agreement if there are any virus or other such technical threats to its internal systems as a result of external email traffic.

By signing below the patient indicates they have read an understood the conditions given above. The patient also understands they are able to review or cancel this arrangement at any time in writing.

Name _____

Address _____

Signature _____

Agreed on behalf of XXXXXXXXXXXXXXX Trust

_____ signature

_____ designation

Glossary of Terms

Confidential information:	<p>This includes ‘Person Identifiable’ information, ‘Sensitive Person Identifiable’ information, and ‘Business Sensitive’ information.</p> <p>[Language around confidential information varies depending on the originator. The Data Protection Act uses the terms: ‘Personal’ information and ‘Sensitive Personal’ information. Health tends to use the terms ‘Person Identifiable’ information, ‘Sensitive Person Identifiable’ information and ‘Business Sensitive’ information <i>NHS Connecting for Health, IG Toolkit</i>]</p>
Person Identifiable information:	<p>This is information that relates to a <i>living individual</i> who can be <i>identified from that data</i>, or, from that data and any other information which is in the possession of, or likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any intentions of the data controller or any other person in respect of the individual. It includes information that identifies a patient. Key identifiable information includes:</p> <ul style="list-style-type: none"> • Person’s name, address, full postcode, date of birth • Private email, home phone number • Pictures, photographs, videos, audio-tapes or other images of patients • NHS number and local patient identifiable codes • Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analysis which have very small numbers within a small population may allow individuals to be identified • Patient Health Records, passports, driver’s licence
Sensitive Person Identifiable information:	<p>This is information that contains details of that individual’s: health or physical condition; sexual life; ethnic origin; religious beliefs; political views; criminal convictions and the following:</p> <ul style="list-style-type: none"> • Mother’s maiden name • Bank / credit card / financial details • National insurance number • DNA or finger prints • Tax, benefit or pension records • Health records • Employment record • School attendance or records • Material relating to social services including child protection and housing
Business Sensitive information:	<p>This is information which if disclosed could harm or damage the organisation’s reputation and image.</p>

Incident:	An information governance incident can include loss of confidential information, breach of confidentiality, and non-compliance with Trust policies.
Anonymised:	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.
Pseudonymised:	This is like anonymised information in that, in the possession of the information holder, it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
Clinical Audit:	A quality improvement process that seeks to improve patient care and outcomes through systematic review of care against explicit standards and the implementation of change (<i>Principles for Best Practice in Clinical Audit</i> , NICE 2002)
Explicit or Express Consent:	This means patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, given orally or in writing, and freely given in circumstances where the available options and the consequences have been made clear.
Implied Consent:	This means patient agreement that has been signalled by behaviour of an informed patient.
Disclosure:	This is the divulging or provision of access to data.
Healthcare Purposes:	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities
Information Sharing Protocols:	Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes:	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001 explicitly broadened the definition to include social care.
Public Interest:	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the

potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services

Social Care:

Social care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes “pure” health care (hospitals) and community care (e.g. district nurses), but may include items such as respite care. There is therefore, no clear demarcation line between health and social care. Social care also covers services provided by others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).

Email Good Practice Guidelines

In order to avoid or reduce the risks set out above for email use within your organisation, the following rules are necessary:

- A. Be aware that the name of the organisation is connected to each email that you send. Every employee is responsible for maintaining the organisation's image and must use email in a professional manner to avoid placing the organisation at risk from legal liability based on email content.
- B. Particular care should be taken when sending person identifiable or business sensitive information. Staff should be aware of the Email Tiers in Appendix 3.
- C. Extra caution needs to be taken with email messages in respect of any disparaging remarks that may be contained therein. Avoid using email for sensitive or emotional messages. Re-read messages prior to sending to check for clarity and ensure that they do not contain anything that could embarrass the individual or organisation, or make the organisation liable. Care should be taken when forwarding an email to delete any part of the original email string that is not relevant or could cause offence.
- D. An email should be regarded as a written formal letter, the recipients of which may be much wider than the sender intended, hence any defamatory or careless remarks can have very serious consequences as can any indirect innuendo. Do not use indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise.
- E. If you receive any offensive, unpleasant, harassing or intimidating messages via email, you are requested to inform your manager or the ASP Service Desk immediately. These emails could contain swear words, words of a sexual nature, "do this or else" or racial abuse etc. It is important that we trace such emails as quickly as possible.
- F. Important or potentially contentious communication, which you have received through email, should be either printed with a hard copy kept (e.g. confirmation of order etc.) or permanently stored electronically outside of the email system.
- G. Do not subscribe to electronic services or other contracts on behalf of your organisation unless you have the express authority to do so. Authority for subscriptions, including electronic subscriptions, rests with a delegated person / position within the organisation and unless you are one of these delegated persons you have no authority to enter into any binding commitment on your organisation's behalf.
- H. Excerpts from reports other than our own, if substantial, may be in breach of copyright and the author's consent ought to be obtained particularly where taken out of its original context. Information received via email should not

be released to another person/organisation without prior consent of the original sender. If in doubt, consult your manager.

- I. On no account should individuals send or forward virus warnings to other users unless instructed to do so by ASP IT Support as some are hoaxes, which just causes unnecessary extra mail. In the event that a user suspects a virus infestation they must stop using that machine and contact the ASP IT Service Desk immediately. Please be aware that some viruses are hoaxes and ask you to delete system files, which can disable your PC or make them less secure.
- J. Employees are not permitted to read emails that are not addressed to them unless by mutual agreement for business continuity purposes to cover for absences. Email messages should be treated as confidential by other employees and accessed only by the intended recipient, (although the organisation has the right to retrieve and read all email messages).
- K. At all times when you leave your workstation you must 'lock' the workstation to stop other unauthorised individuals gaining access to your email. (*To lock and unlock your workstation press down the Control, Alt, Delete simultaneously.*)
- L. Password sharing so others can gain access to your email, and logging in as another user to send email as them is fraud, and a breach of this policy and the Information Security Staff Policy, and is a disciplinary issue up to and including dismissal.
- M. An appropriate subject heading should be used for each email. For personal emails the word 'Private' or 'Personal' should be put in the subject heading.
- N. Staff should be aware when using distribution lists available on the Exchange mail server global address book that these can contain other lists of recipients and could be hundreds if not thousands of email addresses. Inappropriate or careless use can cause serious resource and performance problems with email systems and networks. Check that the list contains only the recipients you need (*Right click on the list name and check 'Properties' which lists all names that will be used for that distribution list*). Inappropriate use of email distribution lists wastes both network resources and staff time, for this reason they are to be used solely for distributing information which is relevant to everyone on the list. The size restriction on sending a single email is 20Mb. Sending of emails with large attachments can adversely impact the performance of the network.
- O. A group email is the most efficient way of sending the same information to a number of addresses but usually this makes it possible for all the recipients to be able to see each other's email addresses. Before sending group emails, consider carefully whether the intended recipient's email addresses should remain confidential to all others belonging to the contact group. Permission to share an email address may not have been given. Staff are advised to put **their own** email address in the "To" box and add all the **intended recipients' addresses** in the "Bcc" box. This will mean that the recipients can see only your address and all other email addresses will remain confidential.

- Patient / person identifiers should be removed wherever possible, and only the minimum necessary information sent.
- Special care should be taken to ensure the information is sent only to recipients who have a “need to know “; always double check you are sending the email to the correct person/s.
- When sending any person identifiable or business sensitive information staff must use nhs.net.

Email Security Tiers

- NHSmail is the brand name for what we call nhs.net email. They are the same thing. **Nhs.net is the only BMA and Department of Health approved email service for securely exchanging clinical data between NHS organisations** (*NHS Connecting for Health*).
- Nhs.net must be used by NHS staff when sharing person / patient identifiable or business sensitive information via email. The recipient's email address must be either nhs.net or one of the government domains listed below.
- All external NHS Trusts should send sensitive and person identifiable emails to our nhs.net accounts only.
- Never guess someone's nhs.net address. Double check you have the correct address either by phoning the person or using the nhs.net directory.
- Email addresses given out to the public on publicity material or on websites as part of formal public engagement work (e.g. audit, consultation, complaints, research) should be nhs.net addresses not PCT email addresses.
- No person identifiable or business sensitive information, should be sent to a public Internet address like firstname.surname@hotmail.com
- Do not forward work documents to your home email address or public Internet address for remote working. If you have a remote working requirement you should use an encrypted Trust laptop and NHS secure access token.
- Please report all incidents relating to IT security, information governance and confidentiality to the Risk Manager and Information Governance Manager. See the Incident & Near Miss Reporting Guidance on the NHS Cambridgeshire website.
- For full guidance please refer to the Email Acceptable Use Policy. This can be found at www.cambridgeshirepct.nhs.uk.

When sending confidential information via email, you need to consider the most appropriate Security Tier versus the urgency that the information is required. The sender remains responsible for making the decision on the type of email address used. The following email options are available ranging from Tier 1 the most secure, to Tier 5 the least secure:

Tier 1 Source: nhs.net Destination: nhs.net

Example: **John.Smith@nhs.net** to **Fred.Bloggs@nhs.net**

Use: This is the account that must always be used for sending person/patient identifiable or business sensitive emails safely between nhs.net users. Emails sent nhs.net to nhs.net are encrypted.

Tier 2 Source: nhs.net Destination: Government Organisation

Example: **Emma.Smith@nhs.net** to **Another.Person@gsi.gov.uk**

Use: This type of email account must always be used for sending person identifiable or business sensitive emails to a third party, where the recipient has a legitimate need to know, does not have an nhs.net address, but has one of the addresses from the domains listed below.

.gsi.gov.uk	.gcsx.gov.uk	.mod.uk
.gsx.gov.uk	.cjsm.net	.scn.gov.uk
.gse.gov.uk	.pnn.gov.uk	.pnn.police.uk

.gsisup.co.uk

.eu-admin.net

.police.uk

Emails sent via nhs.net to the above domains are encrypted between your PC and the above government domain addresses so the content does not need to be encrypted. Only messages sent to these *specific* domain users can be guaranteed safe and secure at this time.

Tier 3 Source: nhs.uk Destination: nhs.uk

Example: **Emma.Smith@trust-pct.nhs.uk** to **Another.Person@trust-pct.nhs.uk**

Use: This type of email account is for day-to-day business but should not be regarded as secure and therefore should NOT include the use of person identifiable or business sensitive emails.

Tier 4 Source: nhs.uk Destination: cambridgeshire.gov.uk*

Example: **First.Surname@trust-pct.nhs.uk** to **First.Surname@cambridgeshire.gov.uk**

Use: By special arrangement with Cambridgeshire County Council, email sent from an ASP IT Partner to @cambridgeshire.gov.uk is sent via a direct link. This prevents the email from traversing the Internet. However, it should NOT be used for person identifiable or business sensitive email information. NB This only applies to Cambridgeshire County Council using a cambridgeshire.gov.uk address.

Tier 5 Source: nhs.uk or nhs.net Destination: .co.uk, .com, .net

Example: **Emma.Smith@trust-pct.nhs.uk** to **johnny45@hotmail.com**

Use: This is the least secure type of email, as they are sent across the Internet. Under NO CIRCUMSTANCES should any business or person identifiable information be sent to these addresses.

SECURE EMAILING

When you wish to send emails that contain, or have attachments containing, confidential or person identifiable information, it might be helpful to use the grid below to check which routes are secure.

From ▼ / To ►	Nhs.net	Government domains (see Tier 2 list above)	PCT	Other networks	Hotmail / Yahoo internet email
Nhs.net	Secure	Secure	Not Secure	Not Secure	Not Secure
PCT	Not Secure	Not Secure	Not Secure	Not Secure	Not Secure
Home / personal email account	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited