NHS

EMAIL POLICY

Policy approved by:	Audit & Governance Committees
Date:	July 2018
Next Review Date:	July 2019 (1 year review date as a new policy)
Version:	1.0

CCGs working together

Airedale, Wharfedale and Craven CCG
Bradford City CCG
Bradford Districts CCG

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Officer
Clinical Lead:	Caldicott Guardian
Author:	Senior IG Specialist, eMBED
Date Approved:	13th July 2018
Committee:	Audit and Governance Committees
Version:	1.0
Review Date:	July 2019

Version History

Version no.	Date	Author	Description	Circulation
0.1	24 October 2017	Senior IG Specialist, eMBED	Initial Draft Policy	Senior IG Specialists within IG Team, eMBED
0.2	13 November 2017	Senior IG Specialist, eMBED with input from Stephen Petty	Draft Policy with IG Team input	Stephen Petty, Head of Service Desk, eMBED
0.3	18 January 2018	Senior IG Specialist, eMBED with input from Stephen Petty	Draft Policy with IG and IT input	Sarah Dick, Head of Governance
0.4	19 January 2018	Senior IG Specialist, eMBED with input from Stephen Petty and Sarah Dick	Draft Policy with IG, IT and Head of Governance input. Draft Policy approved by A&G Comms 12th Feb 2018 subject to review by the HR Partnership Forum (approved)	Fiona Jeffrey, Simon Wilson, Audit & Governance Comms
0.5	July 2018	Simon Wilson, Head of IT	Addition of policy statement on email access via personal devices	A&G Committees
1.0	July 2018	As above	Version approved by July A&G Committees	CCG wide – via Staff Bulletin and M Drive

Contents

1. INTRODUCTION

NHS Airedale, Wharfedale and Craven Clinical Commissioning Group, Bradford City Clinical Commissioning Group and NHS Bradford Districts Clinical Commissioning Group (hereafter known as the CCGs) recognise that the use of email is a popular and important method of both internal and external communication and its use is of great benefit to the operation of the organisation. There are, however, risks associated with the use of email relating to security, confidentiality and content.

The policy set out the parameters for correct email usage and aims to ensure any potential risks are addressed.

2. AIMS

The aim of the policy is to ensure that:

- Employees understand their obligations and responsibilities with regard to use of email**.**
- Employees understand how certain legislation, such as the General Data Protection Regulation (GDPR) 2016/679 and Data Protection Act 1998, places obligations on the CCGs and their employees as to how information held by the CCGs can be used.
- Assurance is provided to the Governing Bodies that the CCGs have in place the processes, rules and guidelines to ensure information is dealt with legally, efficiently and effectively.
- Direction is given to staff in the effective and appropriate use of email.
- Working in accordance with the NHS Mail Acceptable Use Policy

3. SCOPE

This policy must be followed by all staff who work for or on behalf of the CCGs including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and commissioning support organisation staff working for the CCGs. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

The policy applies to all CCG email accounts that are used on CCG and non-CCG premises including from home, internet cafes and via portable media such as Laptops, iPads and smart phones. The policy also governs personal email accounts accessed from CCG systems.

4. ACCOUNTABILITY AND RESPONSIBILITIES

There are a number of key Information Governance roles and bodies that CCGs need to have in place as part of its Information Governance Policy and Framework, these are:

- Audit and Governance Committees
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owner
- Information Asset Administrator
- Heads of Service
- All employees

The accountability and responsibilities of staff are set out in more detail in the Information Governance Strategy and Strategic Vision which must be read in conjunction with this policy.

All employees are personally responsible for compliance with the law in relation to their use of email that involves the use of work derived information. More specific user requirements in terms of email are outlined in sections 8, 9 and 10 of the policy.

All Managers are responsible for ensuring that the staff they manage are aware of this policy and of their individual responsibilities in respect of this policy.

All staff are responsible for reporting information incidents and near misses including breaches of this policy, using the CCG Incident Reporting Policy and Procedure.

5. RISKS ASSOCIATED WITH EMAIL

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal and non-legal risks of email which include:

- If you click a link that inadvertently opens the CCG network to cybercrime.
- If you send or forward emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the CCGs can be held liable.
- If you unlawfully forward confidential information, you and the CCGs can be held liable.
- If you send an attachment that contains a virus, you and the CCGs can be held liable
- Emails can be legally binding and an individual could inadvertently enter the organisation in to a legal arrangement such as a contract.

By following the guidelines in this policy, the email user can minimise the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and may be subject to disciplinary action by the CCGs.

Some of the key legislation and common law is set out in section 13 and how it may affect use of information for email communications. Employees need to be aware of legal requirements for both work, and for personal use (where it may have an impact on the CCGs).

6. ACCESS TO EMAIL

CCG staff who do not handle or have access to Patient Confidential Data (PCD) will have a local email account that ends in @awcccg.nhs.uk or @bradford.nhs.uk.

CCG staff who handle Patient Confidential Data (PCD) must have a national NHS mail account e.g. @NHS.net. Some staff may have other accounts such as a local government email account.

The address for NHSmail email accounts ends in @nhs.net and can be accessed from anywhere via the Internet. NHSmail is a secure email system which encrypts email content during transfer where the recipient and senders are using nhs.net email addresses.

There is a formal, documented user registration and de-registration procedure for access to the network. All requests should be submitted via the IT Self service portal.

The CCG does not condone the access of work emails from personal devices as we are unable to remotely manage and guarantee security compliance. Should you decide to do this for your own convenience then you must ensure, as a minimum, implement a screen lock code and keep your mobile phone / device operating system up to date.

7. EMAIL SECURITY

7.1 Sending Emails Containing Personal Confidential Data

Where personal, confidential or sensitive information is to be sent via email, the content must be secure and only use an encrypted method of transfer. Email may be used to transport a small amount of data (under 20MB).

The email must be sent securely. Sending from NHSmail to NHSmail (i.e. between email addresses ending in @nhs.net) is secure.

When sending emails to any other domain than nhs.net, staff must place the [secure] prefix as the first word with brackets in the email subject field. This will secure the email by activating the NHSmail encryption tool.

Guidance is available on the NHSmail website

The subject header of an email communication must not contain personal or confidential data. Emails must only contain the minimum amount of identifiable information required. Before sending an email, the recipient's details must be verified with particularly attention paid to the organisation that the individual is based in. This can best be done by using the Address Book or Check Names function.

Where the sending of personal and confidential data via email for a specific purpose is a regular or standard occurrence e.g. Individual Funding Requests, patient transport, personalised commissioning, safeguarding – it must be recorded as such on the CCGs Information Asset Register and Data Flow Map, outlining the security methods used and legal basis for such a transfer.

Please contact the Governance Team or the eMBED IG Helpdesk at eMBED.infogov@nhs.net for information and assistance with the Information Asset Register or Data Flow Map.

7.2 Sending and Receiving Emails to Individuals

Staff may receive emails from individuals such as service users, complainants or a member of the public in which the individual may have included sensitive personal and confidential information relating to the complainant or another individual. Without having security such as encryption, an email is an unsecure means to communicate and emails sent to and from an individual's home email will most likely not be completely encrypted during transfer.

Where this is the case, when responding to the original email staff need to inform individuals about the nature of email communications. In all further communications with individuals which may relate to confidential sensitive personal information, staff need to be certain as to the identity of the individual and that they have relevant consent to process such information. Where staff communicate by email they must use the NHSmail encryption tool ([secure] in the email subject) when sending to non nhs.net addresses Care should be taken in the drafting of responses and anonymise or minimise any personal and confidential information
(see: Anonymising emails in Appendix A).
.

7.3 Storage of Emails Containing Personal and Confidential Data

When saving emails containing personal and confidential information they must be saved in a secure location i.e. on the organisational network drives and with protection appropriate to their sensitivity. Emails containing either patient or staff identifiable information must be stored on an access restricted folder on a secure network drive, they must not be stored at any point on computer desktops or local hard drives e.g. C: Drive.

7.4 Email Security at Home and Out of the Office

Staff using work email accounts at home or within other out-of-office settings need to ensure the security of the email so that other individuals cannot access or view them. The **Information Security Policy** sets out security standards in the work environment.

7.5 Email Access via Personal Devices

The CCG does not condone the access of work emails from personal devices as we are unable to remotely manage and guarantee security compliance. Should you decide to do this for your own convenience then you must ensure, as a minimum, implement a screen lock code and keep your mobile phone / device operating system up to date.

8. PERSONAL USE

The email system used by the CCGs is meant for business use. The CCGs Internet and Social Media Policy together with the NHS Mail Acceptable Use Policy outlines acceptable personal usage for Internet related activity such as email.

9. MANAGING EMAILS

9.1 Storage, Retention and Destruction of Emails

To manage email messages appropriately, members of staff need to identify email messages that are records of their business activities as opposed to routine email messages. For example, at the start of a project, an email may include the setting out of key points for staff to consider in setting up a new process, this could be classed as a record and needs to be saved with other documentation relating to the new process. An email confirming that you are able to attend a meeting is routine and would not need to be saved for any length of time.

It is important that email messages and their attachments which are 'records' (see definition above) are moved from personal mailboxes and managed in the same way as other records.

Such emails could be saved to the relevant access folder in the shared drive unless the information is in draft or is confidential, in which case staff should save it in their personal secure area on the appropriate network drive.

The email system itself should not be treated as an information archive.

Staff need to be aware:

- Because emails are another form of record they are subject to Records Management protocols and legislation.
- You must never delete email (or any other type of record) if you know or suspect that it may be subject to a Freedom of Information request (i.e. leading to or documenting any aspect of the decision making process).
- Emails containing important links to projects and processes and/or including decisions should be retained.

Emails should only be retained where there is a legal requirement to do so. The CCGs have adopted the retention periods set out in the Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

For further information about emails as records, staff need to read the CCG **Records Management and Lifecycle Policy.**

9.2 Staff Absence

9.2.1 Planned Absence

In the case of planned absence from work, staff should arrange with their line manager for delegate rights to be set up by IT where appropriate. Before planned absence commences, staff must set an automatic response to ensure that the sender of the message is informed that emails will not be read or acted upon until the staff member returns or that the sender can contact another staff member about their sent email.

There may be circumstances where emails of an absent staff member (even on planned leave) may need to have some of their emails responded to (for continuance of business purposes) while they are away. Such an arrangement will need the authorisation of a Director. The member of staff must be informed of the delegated access and advised when such access has been revoked (which should be no later than when the staff member has returned to normal duties). The headings of emails should only be viewed in most cases and only when the heading indicates that an email requires a response (and/or that the email has been sent from a person who the covering staff member has been directed to provide a response to) can content be read. Any emails with the subject "Personal" or "Private" should not be viewed. Advice on access to another staff member's email can be obtained from the NHS Mail help and guidance webpages or IT service desk (see Section 18: Advice).

9.2.2 Unplanned Absence

In cases of unplanned long term absence (e.g. through sickness), Line Managers can ensure that the email for absent staff for continuance of business purposes can be read and dealt with by another staff member through the use of proxy access or forwarding by obtaining written authorisation by a Director. There must be a record of when the member of staff concerned was informed of the delegated access and then advised when such access was revoked (which should be no later than when the staff member has returned to normal duties). Any emails with the subject "Personal" or "Private" should not be viewed. This can be facilitated through the IT service desk after discussions and authorisation by the appropriate manager(s) (see Section 18: Advice).

9.3 Closing Accounts

When a member of staff leaves the CCGs, their Line Manager must inform IT Services that they have done so. If they have an organisational account it must be marked as a leaver. The status of the NHSmail account will be dependent what the staff member's arrangements are after they leave the CCG, if the account is to be reinstated, the individual must join a new NHS organisation within 30 days.

9.4 Attachments

Avoid sending large attachments if at all possible, especially to multiple email addresses, as this can cause network congestion and storage space issues. Where possible include a link to a document instead of attaching the document.

A large file is anything over 3MB in size. Avoid sending emails with scanned images inside them or large pictures. Also refrain from cascading large multiple attachments.

The current NHS Mail email limit is set at 20MB.

9.5 Content and Etiquette

Email is a useful resource and effective communication tool however it may not always be the best way to communicate information via email as email messages can be misunderstood and the volume of email messages that people receive can be prohibitive to receiving a meaningful reply as a result of email 'overload'.

Normal business language should be used when staff send emails. All staff should be aware of the impact that the language and material they use may have upon the recipients and any others who may come into contact with it. In particular, material of the following nature must not be communicated, copied or displayed:

- Offensive or potentially offensive
- Sexually explicit
- Illegal
- Discriminatory
- Defamatory
- Political propaganda

Additionally, staff must not purposefully or without due diligence:

- Send malicious emails or viruses, 'worms', executable files designed to disrupt the work of the CCGs or email recipients
- Send unsolicited email to multiple recipients, except where it relates to the administrative activities
- Create or transmit material that is abusive or threatening to others, or serves to harass or bully others
- Use email to commit the organisation to a legally binding arrangement that is outside that individuals delegated financial limits or does not follow the organisations standing financial instructions.

For detailed information on content and etiquette see Appendix A.

10. MONITORING OF EMAIL COMMUNICATIONS

The use of email is covered by the NHSmail Acceptable Use Policy, and should be read in conjunction within this policy.

Line managers should monitor staff compliance with the email policy. Concerns should be raised with staff members if they are seen to not be working in accordance with the policy

All emails are monitored for viruses, however staff should be aware that these are not always automatically detected and blocked. The content of emails is not routinely monitored, however, the CCGs reserve the right to retain message content as required to meet legal and statutory obligations, for example to assist with a criminal investigation.

Monitoring of content of a staff member’s emails would only occur where there was a clear suspicion of criminal activity and in accordance with legislative conditions (See Section 13, Related Law).

Access to a staff member’s email may occur to ensure the continuance of business services (See Section 10.2.1. and 10.2.2.) although staff must be made aware of this where this occurs

11. INCIDENT REPORTING

All actual, potential or suspected incidents involving use of email, the internet or social media need to be documented in line with the CCG’s Incident Reporting Policy and Procedure.

An IR1 reporting form should be completed, reviewed and signed by the reporter’s line manager and sent to the Governance Team as soon as possible after the incident has been identified (the IR1 form can be found here: ../../../../Core%20Docs/Templates/Forms/Incident%20reporting]..\..\..\..\Core Docs\Templates\Forms\Incident reporting)

Actual IInformation Governance and Cyber Security Serious Incidents will need to be entered on the Incident reporting module of the Information Governance Toolkit. These will usually be incidents where there is a loss of personal data involving a large amount of individuals or particularly sensitive personal and confidential information has been disclosed without the legal basis to done so or in error.

From the 25th May 2018, information governance and cyber security serious incidents must be reported via the IG Toolkit incident reporting tool within 72 hours of being identified. **Swift reporting is therefore vital.**

12. RELATED LAW

This section sets out key legislation and common law affecting the use of email.

12.1 General Data Protection Regulation (GDPR) and Data Protection Act 1998

Sets out the conditions for the processing of personal information by organisations and individuals. Employees need to be aware that any use of personal information stemming from work related business can only be used where conditions of the General Data Protection Regulation (GDPR) and Data Protection Act 1998 can be met. Organisations are legally required to ensure the security of personal information that they process.

12.1.1 Subject Access Requests

Individuals have the legal right to request personal information that is held on them by organisations processing personal information such as the CCGs. Requests could come from individuals such as service users, complainants, and CCG staff - this is known as a Subject Access Request (SAR). It could be possible that following receipt of a subject access request, that email content that an employee holds and/or has produced could be subject to release as part of a request where those emails contain personal information relating to the individual. Where such a request is received, staff may have to search through their emails and filing systems for any relevant email content for consideration of release.

Further information can be seen in the **Subject Access Request Procedure**.

12.2 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented
- Where disclosure is in the public interest (the needs of the many outweigh the confidentiality concerns of an individual); and
- Where there is a legal duty to do so, for example a court order.

Confidential information could relate to personal information of an individual or information contained in a business related document e.g. a Contract.

12.3 Freedom of Information Act 2000

Allows the right of access to anyone to recorded information held by a public authority (such as a CCG) through either a request for specific information or through accessing information via the Publication Scheme. Release of information is subject to exemptions and conditions of the Act.

Information held on a staff member's email communications may be caught by the Act if they are relevant to a specific request that has been received. In which case, the staff member would need to search for relevant email content and provide that content to the Freedom of Information processing team.

For further information see the **Freedom of Information and Environmental Information Regulations Policy.**

12.4 Human Rights Act 1998

Article 8 of the Act provides a right of privacy for individuals. In complying with the Act, public authorities (to which the Act applies) such as the CCG need to ensure that personal and confidential information is not disclosed unless a legal justification exists to do so.

12.5 Privacy and Electronic Communications Regulations 2003

The Regulations cover:

1. Marketing by electronic means, including marketing calls, texts, emails and faxes. The Regulations specify a clear need for consent when emailing or texting individuals (referred to as subscribers). It should be noted that the definition of 'marketing' is very broad and including seeking to influence individuals' behaviour.
2. The use of cookies or similar technologies that track information about people accessing a website or other electronic service.
3. Security of public electronic communications services.
4. Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (e.g. caller ID and call return), and directory listings.

12.6 Computer Misuse Act 1990

Under this Act it is an offence to have unauthorised access to computer material or to undertake unauthorised modification of programs or data on a computer.

12.7 Copyright, Designs and Patient's Act 1998 (as amended by the Copyright Computer Programs Regulations 1992)

See Section 16: Copyright.

13. TRAINING

There are Information Governance implications involved in the use of email especially in terms of: confidentiality and security, legal use, and access to emails. Therefore, it is important that staff understand their Information Governance responsibilities. The Information Governance Toolkit requires that all staff must undergo Information Governance training annually. The Information Governance Training Strategy specifies the training needs of all staff working for the CCGs. All staff will receive Information Governance training via the CCG Statutory and Mandatory Training Programme. Managers must actively ensure that all staff undertake all applicable and mandatory Information Governance training.

14. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Audit and Governance Committees this policy will be disseminated to staff via the CCG briefing process and will be available on the CCG shared drive.

As a new policy, this policy will be reviewed 12 months following issue. Thereafter this policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

15. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Information Governance Toolkit (IGT), will be undertaken each year. The IGT includes requirements relating to confidentiality, data protection, security of and access to information. Incidents are reported and all serious information governance issues must be reported by the SIRO at Governing Body level and in Annual Reports.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the Report NHS Fraud website or telephoning 08000284060.

16. COPYRIGHT

No member of staff shall infringe copyright in copyright works stored on Internet sites. Staff should note that downloading copyright text or images from an Internet site without permission may constitute infringement of copyright even if it is not the intention to republish such works. Staff must **always** check copyright notices on websites.

17. ADVICE

Advice and guidance on any matters stemming from the policy can be obtained by contacting your line manager or through the IG service provided by Embed: embed.infogov@nhs.net

18. ASSOCIATED DOCUMENTS

18.1 Core Information Governance Polices

This policy should be read in conjunction with:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Integrated Risk Management Framework
- Incident Reporting Policy
- Business Continuity Policy
- Disciplinary Policy
- Anti-Fraud, Bribery and Corruption Policy
- Whistleblowing and Raising Concerns Policy
- Internet and Social Media Policy

18.2 Other Related Documents

- Access to Records Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
- Privacy Impact processes
- Remote Access and Home Working Procedures
- Safe Transfer Guidelines and Procedure
- Incident Management, Investigation and Reporting Procedures
- Contract of Employment (section 26)

19. PUBLIC SECTOR EQUALITY DUTY

The Equality Act 2010 includes a general legal duty to:

- Eliminate unlawful discrimination, harassment victimisation and any other conduct prohibited under the Act
- Advance quality of opportunity between people who share a protected characteristic and people who do not share it
- Foster good relations between people who share a protected characteristic and people who do not have it

The protected characteristics are:

- Age
- Disability
- Gender reassignment
- Marriage or civil partnership
- Pregnancy and maternity
- Race
- Religion or belief
- Sex

- Sexual orientation

Public bodies have to demonstrate due regard to the general duty. This means active consideration of equality must influence the decisions reached that will impact on patients, carers, communities and staff.

It is no longer a specific legal requirement to carry out an Equality Impact Assessment on all policies, procedures, practices and plans but, as described above, the CCGs do need to be able to demonstrate they have paid due regard to the general duty.

This policy sets out how the CCGs ensure that email use is legal. It is not believed that this policy will impact on or affect differently or adversely any of the groups with protected characteristics.

Appendix A: Guidance on the use of email

Email titles

- The subject heading (or title) of your email should be relevant, clear, brief and not contain identifiers this will help you to file, retrieve and prioritise the content of the message.

Email content

- All email message content should be written in lower case. CAPITAL letter can be considered aggressive
- Remember to keep it short and simple - avoid sending lengthy emails with the whole history of a topic if it is possible to do so
- Put different topics in separate emails; don't put them in one long email if you there is a lot of content consider writing a document and sending it as an attachment.
- Care should be taken in the content. Nothing should be said in an email that could not be written in a letter or spoken face to face. Staff need to be aware that emails could end up being disclosed to the public in response to a Freedom of Information / Subject Access or Environmental Information Request.
- Staff should include their name, job title, organisation title and contact details at the end of emails
- Read receipts - when sending an email, requesting a read receipt only indicates a message was opened, not necessarily read, understood and acted upon. Read receipts should not be routinely requested as this increases email traffic volumes. Not all systems will generate read receipts.
- Read through your email before sending it:
  - check your spelling and the layout
  - check that your content is clear and correct
- Do not count on users reading their email every day. Urgent messages like stating you cannot make a meeting are best communicated by phone in the first instance, and only sent by email as a backup.
- Only use the *High importance* level indicator on messages that warrant it.

Addressing and sending your email

- Check recipient details
- Be selective, only send the email to those who really need it
- Take care when addressing email to someone for the first time particularly when using NHS mail which is a national system. Do not assume that the email of the person you want to contact will be firstname.surname@..... When using NHSmail - to ensure you send the message to the correct person you can show the person's organisation next to the email address in the email address box e.g. john.smith4556734445@nhs.net (Bradford X CCG). This can be done by clicking on the icon above *Check Names*

- For NHSmail where you find out the NHSmail address is incorrect or you are not sure of the address you can search for the correct address in *Tools*

- When you have sent your email consider deleting it or placing it in a file for future reference.

Managing your Inbox and attachments

- Process or action your emails as soon as possible
  - Consider putting a reminder to yourself by marking items *urgent* or *flagged* for follow up
  - try not to print emails unless absolutely necessary
- As soon as emails have been actioned either file or delete them
- Keep the number of emails in your inbox down to a minimum
- Deleted items are automatically purged by the system at regular intervals however it is good practice to ensure this that your deleted items are cleared frequently.
- Manage any attachments you receive by either:
  - filing the whole email (including attachments) in your email file system
  - saving either the whole email or the attachment separately in your non email file system to create space in your inbox.

Replying and forwarding

- Please note that attachments are automatically removed when you use *Reply* and included when you use *Forward*
- Always use the Out of Office Assistant if you are going to be away from your email
  - Give the details of anyone who is covering for you
  - Never give away personal information: e.g. that you’re away on holiday

NHSmail email encryption feature: secure email from NHSmail to non-accredited or non-secure email services

The NHSmail email encryption feature should be used where an email contains personal confidential data. If you are liaising with other agencies then you should ensure your emails are anonymised – that any identifiable information relating to patients or other staff is removed.

NHSmail automatically provides a secure method of exchanging sensitive information with other NHSmail users and public sector contacts that use one of the other secure Government email services (see Section 8.1 for a list of accredited domains).

Additionally, NHSmail users can manually securely exchange sensitive information with users of non-accredited or non-secure email services, for example those ending in .nhs.uk, Hotmail, Gmail and Yahoo. This requires the user to follow the NHSmail/NHS Digital guidance to ensure that such emails are encrypted.

Emails containing any Personal Confidential Data (PCD), otherwise referred to as identifiable information, must not be sent from nhs.net to a non-accredited email address without using the manual NHSmail encryption feature. If the recipient is unable to decrypt/open an encrypted email they should be provided with support regarding how to do this (see guidance referenced above). In the event of the individual still struggling to access the email, consideration should be given to other forms of communication. Although it remains acceptable to encrypt and ‘ZIP’ a document to the AES 256 standard, this should only be considered in extraordinary situations.

Email Access via Personal Devices

The CCG does not condone the access of work emails from personal devices as we are unable to remotely manage and guarantee security compliance. Should you decide to do this for your own convenience then you must ensure, as a minimum, implement a screen lock code and keep your mobile phone / device operating system up to date.