NHS
South Warwickshire
Clinical Commissioning Group

Email Usage Policy

VERSION CONTROL

Version:	3.0
Ratified by:	Governing Body
Date ratified:	21/03/2018
Name of originator/author:	Head of Information Governance
Name of responsible committee:	Clinical Quality and Governance
Date last issued:	20/03/2019
Review date:	March 2022

VERSION HISTORY

Date	**Version**	**Comment / Update**
03/04/2013	1.0	Approved by Governing Body.
21/03/2018	2.0	IT Provider's Policy approved by Governing Body.
05/02/2019	2.1	Reviewed by IT provider and revisions proposed.
13/02/2019	2.2	Reviewed and amended by Corporate Governance Manager and Arden & GEM Commissioning Support Unit's Information Governance Consultant.
27/02/2019	2.3	Reviewed by Clinical Quality and Governance Committee.
20/03/2019	3.0	Approved by Governing Body.

Contents

1. Introduction

1.1. Information is a popular method of communication. It is of great benefit to when used appropriately. Its use, however, exposes the Clinical Commissioning Group (the CCG) and individual users to risks. These include legal action due to breaches of data protection and confidentiality requirements, threats to the CCG and information security, and ineffective communication. These risks and threats can compromise the CCGs ability to deliver effective care and services. Consideration should therefore be given to whether it is appropriate in any given situation to communicate by email.

1.2. All emails may be subject to disclosure under the Freedom of Information Act 2000 or Data Protection Act 2018. This policy should be read in conjunction with the Freedom of Information Policy, Access to Health Records Policy, Confidentiality and Data Protection Policy and Subject Access Request Procedure.

2. Purpose

2.1. The purpose of the policy is to aid the effective and appropriate use of email on the CCG systems and to reduce the risk of adverse events by:

- Setting out the rules governing the sending, receiving and storing of email;
- Establishing user rights and responsibilities for the use of its system;
- Promoting awareness of and adherence to current legal requirements and NHS information governance standards;

2.2. This policy applies to the use of CCG email and NHS email accounts for business purposes using IT equipment.

3. Definitions

3.1. **Users**

All staff and anyone using or accessing email on behalf of the CCG.

3.2. **Secure Methods of Email**

Secure Methods of email must be used when emailing personal confidential data (PCD) / person identifiable / sensitive / confidential information by email.

Please refer to Appendix 1 for a list of secure email routes.

3.3. **Encryption**

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right password to unscramble it. Encryption software turns text into code format, therefore undecipherable.

3.4. **Sophos Encryption**

A type of email software used to encrypt emails. This encryption is now available to all staff using southwarwickshireccg.nhs.uk email accounts in Outlook. The selection of the Sophos Encrypt button prior to sending the email will ensure that it is encrypted during transit to recipients.

3.5. **Information Breach**

A breach or potential for a breach of information that is either personal / personal Confidential data / sensitive (including commercially sensitive) and confidential. Information breaches may be escalated to a Serious Incident.

3.6. **Non-CCG or Personal Equipment**

Any piece of equipment that has not been supplied by the Corporate IT provider (the provider) i.e. your own personal equipment such as your home computer, laptop or smart phone.

3.7. **Personal Information**

This is information that relates to an individual person.

3.8. **Personal Confidential Data**

Personal Confidential Data (PCD) is information that if used alone or together with other information would identify a living individual i.e. name, address, date of birth, NHS number etc.

3.9. **Sensitive Information**

Sensitive Information includes Special Category Data and organisationally sensitive data.

Special Category Data

Special category data is personal data which is more sensitive, and so needs more protection. It includes Information becomes sensitive if it includes any of the following types of information about an identifiable, living individual:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Organisationally Sensitive Data

Organisationally sensitive data is information that could affect the commercial standing or reputation of SWCCG. For example, corporate information could include planning reports, end of year accounts prior to being published/approved etc. this information is referred to as 'commercially sensitive' information.

4. Roles and Responsibilities

4.1. The CCG's Accountable Officer has ultimate accountability for ensuring the CCG has principles in place for the use of email, ensuring personal and sensitive information is managed appropriately via this method of communication.

Responsibility for ensuring the CCG has systems and processes in place has been delegated to CCG's Chief Strategy Officer.

4.2. The CCG's Chief Strategy Officer is responsible for ensuring:

- ensuring processes are in place to ensure email is used appropriately and that personal and sensitive information sent via this method is done so in a secure manner;

- the provider provides adequate systems to ensure email can be used and encryption software is available and that monitoring of emails is undertaken and inappropriate use is identified.

4.3. The Senior Information Risk Owner (SIRO) role is performed by the CCG's Chief Strategy Officer. As SIRO they are responsible to the CCG's Governing Body and Accountable Officer for reporting information security risks.

4.4. The Corporate Governance Manager is responsible for:

- receiving and reviewing performance reports (detailing any information breaches via email). Where non-compliance is identified, this will be discussed with the Chief Strategy Officer and appropriate action will be agreed and monitored;

- establishing good practice for the management of PCD and sensitive information, and reporting serious information risks to the SIRO.

4.5. The provider's IT Department is responsible for the hardware (all equipment used), software and network connections used in relation to the use of email. The provider's IT Department will also monitor the use of emails and where inappropriate use is identified this will be reported to the Corporate Governance Manager.

4.6. The CCG's Caldicott Guardian is responsible for ensuring that the SWCCG is compliant with the confidentiality requirements of the Data Protection Act 2018.

4.7. Coventry and Warwickshire Information Governance Steering Group (IGSG) is responsible for the implementation of the Information Governance work programme. Compliance reports will be received and reviewed and where non-compliance is identified action will be agreed and monitored by the IGSG.

4.8. The CCG's Corporate Governance Manager is responsible for ensuring procedures are implemented to ensure the safeguarding of information. They advise the IGSG on non-compliance and provide advice and support to staff as required.

4.9. The Data Protection Officer (DPO) is responsible for informing and advising the organisation and its employees of their obligations pursuant to the GDPR and national data protection legislation, and monitoring compliance, reporting to the highest management level of the organisation – i.e. board level.

4.10. Every staff member is responsible for ensuring they comply with this policy. Inappropriate use of email may result in disciplinary action.

All staff have a duty to report any actual or potential information security incidents in accordance with the CCG's Incident Reporting Policy.

All employees of the CCG should be aware that emails may be the subject of disclosure under Freedom of Information Act 2000 or the Data Protection Act 2018. These disclosures will be managed by the CCG's Freedom of Information Policy, Access to Health Records and Confidentiality and Data Protection Policy which contains the CCG's policy on Subject Access Requests.

5. Process

5.1. Email Accounts

All staff will be issued a CCG email account. This email must be used to send and receive all work related email correspondence.

Some staff will also have access to an NHS.net email account which can also be used for work purposes.

5.2. Access to Email Systems

The CCG provides access to email systems to staff and authorised non-CCG employees only for use as follows:

- Work duties;
- Work related educational purposes;
- Work related research purposes;
- Reasonable and occasional personal use provided that it is done during designated breaks such as lunch times other break times and when other communication methods are not practicable i.e. emailing someone to say that you have been delayed.

Staff must take care not to send CCG data or information to non-work related email accounts or via insecure routes, particularly where the data is PCD and/or sensitive information.

Staff must not set up automated diverts to non-CCG email accounts, specifically home/personal email accounts. Such diverts would be active for all incoming emails, which should they contain personal confidential data and/or sensitive health data they would be automatically forwarded via an insecure route, which could result in an information breach.

Staff need to recognise that any email sent from a work account is sent under the auspices of their employment/professional role and thus should be written as such; staff should be aware that such e-mails could be subject to a Freedom of Information Request, regardless of who it is sent to and for what purpose.

The expectation is that staff will conduct themselves in a professional manner whilst using a work email address and thus the use of unprofessional language or details of unprofessional activities must not be used in any emails sent to or from a work e-mail address. Also the use of the email system should not be used to promote private or other personal/professional business such as private clinical practice or other goods or services.

All new staff will receive email usage training on commencement as part of the New Starter Induction Programme, where login details will allocated.

Non-CCG employees who require access to CCG email systems will be required to complete the IT request form signed by their manager.

The inappropriate use or abuse of email may result in access being withdrawn or amended and disciplinary action being taken.

The provider reserves the right to remove or amend access to the email system at any time in order to protect and preserve the integrity and confidentiality of the system.

5.3. Access to Other Users Email Accounts

Users must not access / use another user's email account by sharing login details and passwords.

Users should be aware that access to their email account by authorised individuals may be necessary in periods of absence for business continuity reasons or for investigation purposes i.e. where the CCG has reason to believe inappropriate use has occurred or there are related legal proceedings.

Where access is required for these reasons the CCG procedures for gaining access will be adhered to and this includes Chief level sign off to allow authorised staff access.

Staff may require others to have access to view their inbox and send emails on their behalf – this must not be done by sharing login details or passwords. The CCG procedures must be adhered to by setting permissions through the delegates' options within the email settings.

Where shared departmental / central email accounts are required, these must be setup by the provider's IT Department, which will ensure the appropriate access rights have been set.

5.4. Sending Emails

- Users should use email only when it is appropriate to do so and not as a substitute for verbal communication.
- Emails should be worded with care because voice inflections cannot be picked up and it can be difficult to interpret tone.
- Email messages must not include anything that would offend or embarrass any reader or would embarrass the CCG if it found its way into the public domain.
- Emails should be composed on the assumption that they may be read by others, particularly people who do not normally work the CCG such as temporary staff/patients and/or carers. Email is easily forwarded and may be read by unintended recipients.
- Emails must be treated with the same level of attention that is given to sending formal letters and memos.
- Email messages should be short and attachments not excessive.
- Users should not use email as the only method of communication if an urgent response is required.
- Where important information has been sent by email, confirmation of receipt must be obtained either by email or by a follow up telephone call.
- Users must access email regularly and respond to messages in a timely manner.
- Users should indicate when they are not able to read their email (for example, when on annual leave) using the tools within the email system and providing out of office contact details as appropriate.

- Inappropriate use of email may result in poor communication, impede the function of the network system, impede the effective functioning of email, or compromise the security of the system.

The following must be included in all emails:

- Subject Heading - A concise meaningful title must be put in the subject heading of every email to indicate its content.

- The CCG's official signature – This must include the user's name, designation, CCG name, contact details and the CCG's current banner. A template signature can be imported and amended using the Signature Settings.

- Disclaimer - This is setup automatically for covwarkpt.nhs.net accounts when the email is to external recipients. Users must only use a disclaimer that has been authorised by the CCG.

- Out of Office message - the 'Out of Office' function must be used when you will be unable to respond to your emails. Out of office messages must include a timescale for when you will pick your emails up and where possible another point of contact.

5.5. **Sending PCD and Sensitive Information by Email**

Confidential, personal or sensitive information must only be sent by email using secure methods.

5.5.1. Secure Email Methods:

A list of secure email addresses is provided in Appendix 1.

5.5.2. Sophos Encryption Facility

All staff must consider whether or not it is appropriate to use the Sophos encrypted email facility when sending emails containing confidential, personal or sensitive information data to recipients external to the CCG.

To use the Sophos encryption facility, staff can use the usual CCG email accounts and when sending to an external or different email account the encrypt button (Sophos) must be highlighted by clicking on it. This will send a message to the recipient to let them know that they are being sent an encrypted email and give them instructions as to how to access the encrypted email.

5.5.3. Emailing Members of the Public, Patients and their representatives

Some individuals may request that communication is done via email. The CCG's website must therefore, include a disclaimer which advises people contacting the CCG by email to use the minimum amount of personal information needed to identify themselves and/or others as the confidentiality and security of any information exchanged via email cannot be guaranteed and to be aware that the CCG has no control, or responsibility, over personal information stored by a person's own Email Service Provider.

Should it be deemed appropriate or requested by the person contacting the CCG, Sophos Encryption may be utilised.

CCG staff must review the appropriateness to engage with individuals via email. For example, staff should make it clear that email is not appropriate if an emergency or otherwise urgent response is required and will not be answered 365 days per week (out of office messages should be updated when staff not available to access emails)

Where applicable, all emails to and from patients and their representatives must form part of their record and this information will be subject to any requests under the Data Protection Act. Thus professional and defensible record keeping principles apply.

5.5.4. Personal Use

CCG email accounts should not be used for personal use except for one-off messages and updates or other urgent communication requirements.

The CCG does not support the use of personal email accounts on its own or its provider's equipment i.e. Hotmail, Yahoo etc.

5.6. Storage, Retention and Disposal of Emails

Email is a communication tool and not a records management system, however some emails may need to be kept as evidence of organisational decision making or will form part of an individual's record. Emails can be and are requested to form part of Data Subject Access requests under the Data Protection Act (staff, patient or public identifiable data and can also be requested as part of a Freedom of Information Request). The use of clear subject identifying information is helpful to locate relevant emails.

5.6.1. Storing Emails

Corporate Records - Where emails provide evidence of actions and decisions made of the CCG's business the user must ensure that these emails are filed in the appropriate place, in either electronic or paper format. These emails form part of the CCG's Corporate Records.

Care Records - where emails provide evidence of decisions made in relation to a patient's care or treatment the user must ensure these emails are filed in the patient's care record.

Staff Records - where emails provide evidence on decisions made in relation to a member of staff users must ensure these emails are filed in the staff personnel file.

5.6.2 Retention and Disposal of Emails

All emails have a retention period that must be adhered to. Refer to the Retention Schedule in the Records Management Policy.

Email accounts should be reviewed by users on a regular basis.

Emails that do not relate to work activities or do not need to be kept as part of a record i.e. chain email, junk emails etc must be deleted as soon as possible after receipt.

Emails deleted by users may not be deleted permanently from the provider's Server.

5.7. Disclosure of Emails

Emails may be the subject of disclosure under Freedom of Information Act 2000 or the Data Protection Act. These disclosures will be managed by the SWCCG Freedom of Information Policy and SWCCG Access to Health Records Policy.

Where emails have been deleted, they are not disclosable; however, emails must not be deleted before they reach there retention period. Where an email has been removed from the email system but a copy filed as a corporate record or as part of the care record copies must be disclosed.

Emails must not be altered prior to disclosure, although they may be subject to exemption/redaction using the exemptions in either the Freedom of Information Act 2000 or the

Data Protection Act depending on the type of data. Advice on disclosure of emails can be obtained from the Information Governance Team.

5.8. **Inappropriate Use of Email**

The CCG will not tolerate behaviour that breaches either the law or general standards of decency and respect. Inappropriate use of email includes, but is not limited to:

- The email system must not be used for excessive personal emails (this is where the email traffic from the user can be shown to have adversely impacted on their work function);
- Use of offensive language and unacceptable tone;
- Harassment, bullying or discriminatory content (tone and content);
- Defamatory content;
- Distribution / forwarding of jokes – this includes any type of joke where the sole purpose of the email is the joke;
- Explicit material;
- Offensive material in any form, whether in the email or as an attachment;
- Distribution of material to any party for whom it was not intended;
- Sending PCD, confidential and sensitive information that has not been suitably encrypted or not using secure email methods;
- Sending PCD, confidential and sensitive information to anyone not authorised to receive that information;
- Sending PCD, confidential and sensitive information to personal email addresses;
- Entering into any form of contract on behalf of the CCG via email, unless the appropriate authority has been given;
- Use of email for personal use or personal financial gain;
- Running/downloading program files (.exe) received via email without the authority of the provider's IT Department;
- Libellous or defamatory statements about any individual, department or organisation (may lead to disciplinary action';
- The compilation, forwarding or distributing of unwanted or unsolicited email (junk email, spam etc);
- The compilation, forwarding or distributing of chain letter type emails;
- Using the email account of another user, with or without their knowledge;
- Sharing you email login details or giving access to anyone else;
- Disparagement of a person in respect of their race, colour, country of origin, gender, gender reassignment, marital or civil partnership status, pregnancy, sexual orientation, age, disability, health, religion or beliefs;

- Undermining the position of another member of staff (or anyone else), such as by circulating jokes, or rumours about them, even when the individual is not the recipient;

- Use of the CCG email for any non-CCG business;

- Using NHS email addresses to register with web sites unless it is directly related to your work / CCG business.

5.9. **Information Risks**

An actual, potential or suspected breach of information / confidentiality must be reported via the CCG's Incident Reporting Policy.
Some examples of breaches could be (these are not exhaustive):

- Email containing personal / sensitive information was received by an unintended recipient;

- Someone has given access to another user's email account without authorisation;

- Personal / sensitive information has been sent by email by an insecure method;

- You receive emails which contain inappropriate content and may also constitute bullying and harassment;

- Your email has been intercepted by someone other than those with authorisation to do so.

5.10. **Security**

All passwords and login details for email systems must be kept confidential. Sharing passwords or login details may result in disciplinary action.

Users must lock their equipment when not with it, for example leaving their PC to make a cup of tea, to attend a meeting or to go for lunch. (To automatically lock the keyboard press the 'windows' and 'L' keys at the same time or press 'ctrl–alt–del' then choose 'lock computer').

All IT equipment that is used for work purposes must be installed with up to date anti-virus and encryption software via the provider's IT Department.

The introduction of viruses and other harmful materials are often as a result of staff opening emails from sources unknown to them. Although the provider's IT Department deploys a wide range of protection software to prevent such harmful material entering its Network via email, there are increasingly sophisticated "scam" emails. If an email is suspected to not be genuine, then it should not be opened; rather it should be deleted from the inbox and from the "Deleted" items area. If a number of "suspect" emails are received, this should be reported immediately to the provider's IT Department.

6. Training

6.1. The CCG will carry out an annual Training Needs Assessment (TNA) and staff are required to undertake relevant training, including mandatory Data Security Awareness training for all.

6.2. The TNA is monitored by the DPO, Senior Management Team and the Audit Committee.

6.3. Email security is included in the Corporate Governance induction for all new employees of the CCG.

7. Equality and Diversity Impact Assessment

7.1. In reviewing this policy, the CCG considered, as a minimum, the following questions:

- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so, is this planned?

7.2. Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy, race, religion or belief, sex, sexual orientation. No adverse impacts have been identified.

8. Monitoring Compliance and Effectiveness of the Policy

8.1. The Clinical Quality and Governance Committee will oversee implementation of the policy and will receive quarterly reports detailing incidents logged, which may include incidents relating to email security.

8.2. The Clinical Quality and Governance Committee reviews the mitigation of information security risks.

8.3. The SIRO will report information security risks, email security breaches to the Governing Body.

8.4. Training data is regularly reviewed by the Clinical Quality and Governance.

8.5. The policy will be reviewed every three years by the Governing Body. Staff will be notified of any key amendments made.

9. References and Further Reading

9.1. Related references and further reading:

- The Data Protection Act 2018;
- The Freedom of Information Act 2000;
- Access to Health Records Policy;
- Confidentiality and Data Protection Policy;
- Freedom of Information Policy;

- Records Management Policy;
- Safe Haven Policy and Procedure;
- Subject Access Request Procedure.

Appendix 1

List of Secure Email Routes

The following email routes are secure:

From:	@pnn.police.uk	To:	@nhs.net
From:	@mod.uk	To:	@nhs.net
From:	@secure.nhs.uk	To:	@nhs.net
From:	@coventry.gov.uk	To:	@nhs.net
From:	@warwickshire.gov.uk	To:	@nhs.net

The following email routes will remain secure until they are replaced with secure @gov.uk email addresses (by March 2019): -

From:	@nhs.net	To:	@gcsx.gov.uk
From:	@nhs.net	To:	@gsi.gov.uk
From:	@nhs.net	To:	@gsx.gov.uk
From:	@gcsx.gov.uk	To:	@nhs.net
From:	@gsi.gov.uk	To:	@nhs.net
From:	@gsx.gov.uk	To:	@nhs.net

Only the email routes listed above are secure.

If you need to send personal data / patient identifiable data to a non-secure email address, advice should be sought from the Corporate Governance Manager.

Blank page

End of Policy