Working with you to make Sheffield HEALTHIER

NHS Sheffield Clinical Commissioning Group

Email Digital Teamworking and Videoconferencing Policy

(Formerly the Email Policy)

January 2021

Version:	5.0
Policy Number:	HR006/01/2023
Date ratified:	29 April 2021
Name of originator/author:	Information Governance Manager
Name of Sponsor:	Deputy Director of Information Performance and PMO
Name of responsible committee	Governance Sub-committee
Date issued:	May 2021
Review date:	January 2023
Target audience:	All staff

To ensure you have the most current version of this policy please access via the NHS Sheffield CCG Intranet Site by following the link below:

http://www.intranet.sheffieldccg.nhs.uk/policies-procedure-forms-templates.htm

MINDFUL EMPLOYER

disability confident EMPLOYER

Policy Audit Tool

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Please give status of Policy:	**Revised**

1.	**Details of Policy/Procedural Document**	
1.1	Policy Number:	HR006/01/2023
1.2	Title of Policy/document:	Email Digital Teamworking and Videoconferencing Policy
1.3	Sponsor	Deputy Director of Information Performance and PMO
1.4	Author:	Gershon Nubour, IG Manager
1.5	Lead Committee	Governance Sub-committee
1.5	Reason for policy/document:	Sets out to staff the appropriate use of email digital teamworking and videoconferencing including the transfer of person identifiable information.
1.6	Who does the policy affect?	All staff
1.7	Are the National Guidelines/Codes of Practice etc issued?	
	Has an Equality Impact Assessment been carried out?	Yes
2.	**Information Collation**	
2.1	Where was Policy information obtained from?	Previous Policy & Information Governance expertise.
3.	**Policy Management**	
3.1	Is there a requirement for a new or revised management structure for the implementation of the Policy?	No
3.2	If YES attach a copy to this form.	
3.3	If NO explain why.	
4.	**Consultation Process**	
4.1	Was there external/internal consultation?	Internal
4.2	List groups/persons involved	IG Group, IG Team, ICS Office365 Lead, IT Dept
4.3	Have external/internal comments been included?	Yes
4.4	If external/internal comments have not been included, state why.	
5.	**Implementation**	
5.1	How and to whom will the policy be distributed?	All CCG Staff
5.2	If there are implementation requirements such as training please detail.	
5.3	What is the cost of implementation and how will this be funded	

6.	Monitoring	
6.1	How will this be monitored	Number of adverse incidents reported Number of complaints received
6.2	Frequency of Monitoring	Monthly

Version Control

VERSION CONTROL				
Version	**Date**	**Author**	**Status**	**Comment**
1.0	July 2014	Information Governance Group		
2.0	July 2016	EMBED IG Team	Review	Personal email accounts removed from scope. CSU references changed to commission support services or EMBED. Counter fraud references added. New NHSMail encrypted email service referenced. NHS Secure File Transfer service referenced. Additional minor changes.
3.0	August 2018	EMBED IG Team	Review	Updated References to DPA/GDPR Staff adherence to NHS Mail policies added. Restrictions on confidential info in calendar appointments added Updated section on emailing securely Spam and Phishing section added Removed instant messaging prohibition Clarified use of Webmail
4.0	January 2021	IG Manager	Review	Renamed and significantly changed and expanded to include new digital ways of working such as Microsoft Teams and Office 365. Reflects changes to NHSMail Removed references to EMBED

Contents

1 Introduction and Purpose

1.1 Email and collaboration tools such as Microsoft Teams are the increasingly dominant methods of internal and external communication for the CCG. Together with the Office 365 system and video conferencing systems, they provide flexible and powerful tools of great benefit to the CCG when used appropriately. Their use, however, also exposes the CCG and individual users to new risks. These include legal action due to breaches of data protection and confidentiality requirements, threats to IT and information security, and ineffective communication. These risks and threats can compromise the CCG's ability to deliver effective care and services. Consideration should therefore be given to whether a chosen tool is appropriate in each particular circumstance.

1.2 Email and other messaging systems are not always the best way to communicate information, as they can often be misunderstood and the volume of messages people receive can be prohibitive to receiving a meaningful reply as a result of communication overload. Emails should be treated with the same level of attention that is given to drafting and managing formal letters and memos. As well as taking care over how email messages are written, emails should be managed appropriately for records management purposes, after they have been sent or received. Messaging through Microsoft Teams is more informal and may feel less permanent, but applying the same care and consideration given to emails, is expected of staff. For all communications systems, take note "out of office" and other status messages as a common courtesy and to ensure effective communication.

1.3 Videoconferencing is an excellent means of arranging meetings establishing and maintaining professional relationships. Care must be taken to maintain a professional attitude during calls and to be mindful that others may not be as comfortable and may find video calls intrusive or disconcerting.

1.4 The Office 365 platform includes other digital collaboration and teamworking tools beyond Microsoft Teams. Onedrive, Sharepoint and others apps provide new ways in which staff can securely store share and process information, with both CCG staff and others. Staff should always be mindful that as internet connected applications which promote sharing, they present a significant risk of confidential information being shared inadvertently.

1.5 This policy sets out the CCG's expectations of staff when using the NHS Mail, digital collaboration tools such as Microsoft Teams, Office 365 and other videoconferencing systems. Accessing non-work email accounts on CCG systems is also addressed.

1.6 Procedures implementing this policy will be made available on the intranet. These documents and the policy itself should be cross-referenced with other related information governance policies and procedures. An up to date list of documents will be made available on the information governance intranet page. Staff should ensure that they are familiar with the content of this policy and use it as a point of reference for digital communications.

1.7 The CCG and wider NHS has embraced the use of Microsoft Teams. It is regarded as secure and is promoted as the default solution when working across organisational boundaries

1.8 The purpose of the policy is to aid staff in the effective and appropriate use of email and digital teamworking to reduce the risk of adverse events by:

- Setting out the rules governing the use and storage of emails, Teams messages, how to use digital collaboration tools safely and expectations regarding the use of videoconferencing.
- Establishing CCG and user rights and responsibilities for the use of its systems.
- Promoting awareness of and adherence to current legal requirements and NHS information governance standards.

2 Scope

This policy applies to:

- NHS email and digital collaboration system accounts for business and personal use on CCG and non-CCG premises and equipment, including from home, internet cafes and via portable devices such as laptops, ipads and smartphones.
- All staff, in particular users of CCG systems and equipment including CCG employees and non-CCG employees who work within NHS Sheffield Clinical Commissioning Group or under contract to it. This includes, but is not limited to, staff on secondment to the CCG, students on placement, commissioning support services staff working on behalf of the CCG and people working in a voluntary capacity.
  (For convenience, the term 'staff' is used in this document to refer to all those to whom the policy applies.)

3 Definitions

CCG	Clinical Commissioning Group
UK-GDPR	UK General Data Protection Regulation
MS Teams	Microsoft Teams
Office 365	Microsoft Office 365 including OneDrive and SharePoint

4 Process/Requirements

Generic Responsibilities of Staff and the CCG

- All managers are responsible for ensuring that the staff they manage are aware of the this policy and their individual responsibility for complying with it. They should ensure their staff are equipped to fulfil those responsibilities; this will include covering it at their local induction and by identifying and meeting specific and generic training needs through personal development plans.
- Managers should ensure ALL new staff have signed the Confidentiality and Information Security declaration. This should be done prior to giving them access to the CCG network. (The requirement to sign the declaration applies to ALL staff who work in the CCG and have access to CCG information and not only those with network access.) Managers are required to countersign this declaration to indicate that they have checked that the member of staff has read the relevant information governance policies and has had an opportunity to ask questions about anything they do not understand.
- Senior managers should ensure that managers within their service are aware of their responsibilities in relation to informing staff about acceptable standards of information governance.

- The CCG allows short communications of a personal nature if it does not interfere with work. Although the personal use of email and other communications platforms is discouraged due to the detrimental effect it may have on CCG business. (See section 7)
- All staff must ensure that they are aware of the requirements and standards of behaviour that apply and adhere to this policy.
- All staff are responsible for reporting information incidents and near misses, including breaches of this policy, using the CCG's Incident Reporting procedures.
- The CCG's incident reporting process can be obtained from line managers in the first instance. Further information can be obtained from the CCG's Risk and Governance Team.
- The CCG's Information Governance Group is responsible for overseeing the implementation of this policy including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

4.1 CCG specific responsibilities and rights

- The CCG provides access to email, digital team working and videoconferencing systems to employees and authorised non-CCG employees only for use in their:
  - Work duties
  - Work related educational purposes
  - Work related research purposes
- No one has a right of access to an the above systems. The inappropriate use or abuse of CCG systems may result in access being withdrawn or amended.
- The CCG reserves the right to remove or amend access to the system at any time in order to protect and preserve the integrity and confidentiality of the system.
- The CCG has monitoring and auditing systems in place to protect against misuse, attack and loss of or inappropriate disclosure of confidential data.

The CCG will:

- Provide users with appropriate training and guidance in the use of email and digital teamworking tools.
- Provide access to systems and resources necessary to carry out their role

4.2 Email - Staff Responsibilities and Rights

- In the first instance Staff using the NHSMail email systems must comply with the NHS Mail Acceptable Use Policy https://portal.nhs.net/Home/AcceptablePolicy
- Staff 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.
- Write ALL emails on the assumption that they may be read by others, particularly people who do not normally work for the CCG such as temporary staff or staff in external organisations. Email is easily forwarded and may be read by unintended recipients.

- Staff must avoid putting confidential information in Calendar Appointments to avoid inadvertent breaches of confidentiality.
- A concise meaningful title must be put in the subject heading of every email to indicate its content
- Where forwarding or replying to emails you must ensure that you are not inadvertently sending personal confidential data, either within the email chain or its attachments
- Users should not use email as the only method of communication if an urgent response is required.
- Where urgent information has been sent by email, confirmation of receipt should be obtained either by email or by a follow up telephone call.
- Staff should access their emails regularly and respond to messages in a timely manner.
- Staff should indicate when they will not be accessing their email using the 'Out of Office' function, listing an alternative contact where possible
- If you are accessing your NHSMail account from a non-NHS device (i.e. personally owned laptop, tablet, smartphone), you should only access the service via the web at www.nhs.net and not through an installed email application such as Microsoft Outlook. This avoids the risk of confidential data being stored insecurely
- Staff must only use disclaimers that have been authorised by the Communications Department.
- Line Managers are responsible for ensuring that e-mail accounts are emptied or closed down as required when staff leave the organisation. This is on the leaver's checklist and should be covered at exit interviews by the line manager who is responsible for informing others by completing the Leavers form. Distribution lists and shared inboxes should be checked as part of the process for leavers.

4.2.1 Sending, receiving and accessing confidential information by email

- Confidential or sensitive information, including information about patients/ service users and staff, must be encrypted if it is sent by email.
- A limited number of email addresses can be regarded as secure and encrypted these include @*.gov.uk and @*.pnn.police.uk. The full list of secure and encrypted email addresses is available here https://support.nhs.net/article-categories/sharing-sensitive-information/
- TO send encrypted emails to other addresses requires placingthe phrase [secure] complete with square brackets, in the subject of the email to be protected. This applies to ALL other email addresses, including @*.nhs.uk ones
  There are a number of other steps which must be followed to ensure confidentiality (such as test messages etc.). If you wish to use this facility you must follow the guidance which is available on the NHSMail portal. *Sharing Sensitive Information:* https://portal.nhs.net/Help/policyandguidance
- Routine transfers of such information must be part of an agreed workflow process and approved by the CCG's Information Governance (IG) Lead. Routine flows of personal information must also be recorded in the dataflows register (see the IG Lead for information).
- Personal confidential data such as names and addresses, should not be included in the subject line of any emails.

- Safe haven procedures[1] must be considered when sending or receiving confidential or sensitive information by email.
- There are several security risks associated with communicating with patients by email. It is difficult to authenticate the identity of patients; communication between the CCG and patients who are using a personal email account or an account from a non-secure domain will not, without additional steps, be secure.
  The CCG should only communicate with patients on matters of a confidential nature if they can verify the identity of the patient and the patient is made aware that email is not a secure method of communication and they consent and accept the risk. Services such as Complaints, who may have routine email contact with patients, should gain IG approval for the process as a whole but not individual communications.
- Access to NHSMail Webmail is allowed from non-NHS equipment, however confidential or sensitive CCG information must not be downloaded and saved on them. Arrangements for working outside of this policy require prior approval from the Senior Information Risk Owner, who will seek advice from the Information Governance Lead.

4.2.2 Sending Large Attachments

- Users should avoid sending or forward large messages or attachments. 10MB should be regarded as the upper limit, but good practice is below 1-2MB. Many email systems will simply block emails larging than 10MB. The sending and storing of large attachments can adversely affect the CCG network. Be mindful of video and presentation files, as they can be quite large.
- Alternatively the new NHS large file transfer system is available: https://support.nhs.net/knowledge-base/egress-large-file-transfer-web-form/
- Where the recipient is available via MS Teams, then that may also be used for transferring large files

4.2.3 Forwarding Email Outside the CCG

- Staff must not automatically forward email from their CCG email account or send confidential or sensitive CCG information to non-NHS email accounts. Examples of non-NHS email accounts include Hotmail, Yahoo, Gmail, and email services provided by internet service providers. Such forwarding should however already be blocked.

[1] The sender should contact the intended recipient prior to sending the email to ensure it will be received in a timely manner (e.g. they are not ill or on annual leave); if it's a shared address that it's appropriate to send the information to it and to ask the recipient confirm its receipt.

4.3 Microsoft Teams - Staff Responsibilities and Rights

- Staff must be mindful that Files and information and made available through MS Teams may remain available indefinitely, depending on how individuals are included in any meeting or chat.

- Staff must also be aware that where any shared files are stored, Typically files for formal Teams are stored in SharePoint, whilst those in standalone meetings, adhoc calls, or chats will be stored in the OneDrive for the person sharing the file.

- It is essential that when staff create or manage a MS Team, that it's is set as "Private" within the Privacy Settings section not "Public". Failing to do so will make it available across the whole NHS, with all the information stored in the Team accessible to all.

- It is also important that a MS Teams meeting created for one purpose is not reused for another, e.g. senior management meeting and then reused for an all staff meeting, leading to risk of inappropriate access to shared messages and documents

- MS Teams is a secure system which can be used to share sensitive personal information. Before doing so please discuss with your line manger or seek IG advice

- Where MS Teams is being used for sensitive or confidential discussions, it is recommended that the anyone not on the original invite is forced to wait in the online lobby before joining.

- Staff should be aware that all documents which are final or form corporate records should be stored in line with what your organisation has decided. This maybe in network drives/ folders or within SharePoint.

- Care must be taken when using Teams on non-NHS devices to avoid downloading and saving information locally. Using the online web versions of Office 365 to view files can help avoid this.

- Teams is not currently suitable for direct patient video consultations where the patient is logging in or controlling one end of the call. The new Virtual Visits application within Office 365 is specifically designed for patient consultations. Please ask for IT and IG guidance if you wish to use this.

- Be aware that MS Teams conversations may be subject to Subject Access Requests and potentially Freedom of Information requests

- Please show with respect and consideration for your colleagues in any messages sent using MS Teams

- Use MS Teams chat for brief and interactive communications, formal communications may still require an email

- If a person has displayed their status as 'Do not disturb', please respect your colleague and do not message them

4.4 Videocalls and Videoconferencing

MS Teams and other videoconferencing solutions are now in common use across the CCG and its partners. Whilst CCG expects them to operate standards similar to actual physical meetings, some additional considerations do exist.

- The participants should confirm at the start of all calls who is present and also acknowledge when a participant joins the call.
- Staff must try to avoid being overheard by having calls in private, particularly when confidential information is being discussed
- Staff should endeavour to attend meetings promptly and also avoid running over.
- Participant microphones should be initially muted especially on “busy” calls.
- Staff are encouraged to switch on cameras during videocalls but are not obliged to, especially when working from home
- All pertinent information arising from the call should be added into the relevant business or patient records as soon as possible after a call. The person(s) responsible for this should ideally be agreed at the start of the call.
- For all calls between colleagues and partners it is good practice and common courtesy to ask if anyone objects to the recording of a call. This provides an opportunity for objections to made and concerns respected and possibly acted upon. This potentially could involve individuals turning off their camera. Alternatively, individuals may wish to withdraw from the meeting.
- Staff should be aware that with recordings the general approach is that they are not the final formal record of information to be kept, and will be deleted when no longer required
- If a decision is made to use call recordings as the main record, then appropriate steps must be taken to catalogue and protect them the same as any other information we hold.
- Obscene or offensive backgrounds, whether real or virtual, are prohibited. Where an external participant has such a background the meeting co-ordinator should take appropriate steps to remedy the situation or terminate the call.
- Where patients (or their representatives) wish to record a meeting using their own equipment then staff should as a matter of routine facilitate this where it is for the patient’s own personal use. Covert recording by patients of their meetings may be regarded as impolite, it is not however prohibited.

4.5 SharePoint - Staff Responsibilities and Rights

SharePoint is a document management system and web portal which allows information to collated and shared as web pages, lists, stored files, databases etc.

- As with other Office 365 apps, any sharing or privacy settings should be set to “Private” not “Public” Only specific groups and individuals should be granted access and use of “Allow everyone in your company” settings should be avoided

- Where there is a requirement for a Sharepoint site which contains confidential information or it is shared with other organisations, please notify the IG Lead as it may need including on the Information Asset Register as well as completion of a DPIA.

- SharePoint Site owners are responsible for the veracity of information stored within it and that access permissions are regularly reviewed.

4.6 OneDrive - Staff Responsibilities and Rights

One Drive is an online internet file storage system. Files stored in it may be synchronised with your PC and vice versa.

- Staff must avoid synchronising or saving data on non-NHS PCs and portable devices (tablets and smartphones) Connecting your NHS OneDrive account to One Drive software on a personally owned device is strictly prohibited
- It is recommended that SharePoint or Teams is used for sharing files with others. It is easier to keep track of who has had files shared with them and ensure that confidential information is managed appropriately.
- As with other Office 365 apps, any sharing or privacy settings should be set to "Private" not "Public" Only specific groups and individuals should be granted access and use of "Allow everyone in your company" settings should be avoided.

4.7 Managing Information and Reviewing Permissions

- Email together with documents shared through MS Teams should be managed and stored in accordance with the CCG's Records Management Policy and other relevant policies.
- Email is a communication tool and not a records management system. Where the content of an email may be needed in the future it is the responsibility of the user to ensure it is stored appropriately (e.g. in network folders or printed out and added to manual records).
- Where the content of an email or attachments forms part of a record, it is the responsibility of the user to ensure the recorded is updated with the additional information, and that it becomes part of that record going forward.
- MS Teams chats may also need to be copied and added to the relevant record
- Emails and attachments that do not relate to work activities or do not need to be kept as part of a record must be deleted as soon as possible after receipt.
- Membership or access to either a Team, SharePoint site, shared OneDrive files and other office365 apps should be reviewed regularly by the owner, with leavers and those who no longer need access or the information, having their access rights removed.
- Line managers and staff must ensure that information stored in personal OneDrive and NHSMail accounts is reviewed to make sure relevant information is stored elsewhere and the accounts cleared of organisational data before any leaving date.

4.8 Legal Requirements

- The use of email and MS Teams must comply with the law such as the Data Protection Act 2018, the UK-GDPR and adhere to CCG rules, codes of conduct, policies and procedures such as this policy and policies relating to equalities and anti-harassment.
- Users must comply with any licence conditions and copyright for any software they have access to.

- Users must not use CCG systems for any purpose that conflicts with their contract of employment.
- Users must not agree to terms or enter into contractual commitments or make representations by email or MS Teams, without having obtained the proper authority. (A typed name at the end of an email is just as much a signature as if it had been signed personally.)
- Emails and MS Teams messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant.
- The content of any messages may be disclosable under legislation such as the Data Protection Act 2018 / UK-GDPR and Freedom of Information Act 2000.
- Improper statements may result in the CCG and/or user being liable under law.

4.9 Security

- All passwords and log in details for email systems must be kept confidential. Sharing passwords or log in details will be considered misconduct.
- Where necessary, staff can give delegate access to their email account. Alternatively, a generic mailbox account can be set up with access via individual email accounts.)
- Users must lock their terminal when not at their computer (for example to make a cup of tea; to attend a meeting; or to go to lunch). To automatically lock the keyboard press the Windows key and 'L' key at the same time  or press Ctrl–Alt–Del, then choose 'lock computer').
- Any computer that is used for work purposes must be installed with up to date, approved anti-virus software. (Advice about anti-virus software can be obtained from the IT Service Desk.)
- Staff who have been assigned wider administrative rights should use the two factor authentication solution provided by NHSMail.
- Only portable devices, including tablet devices, mobile and smart phones, which are encrypted and are able to be remotely wiped should be used to access email.
- Staff should not install additional non-Microsoft Apps available via Office 365 and Outlook without prior approval from the IT Dept.

4.10 Personal Use

- The personal use of CCG messaging systems is discouraged. If it is necessary to use NHS provided systems for personal communications they must be brief, must not detract from the user's work duties and must not disrupt the work of others.
- Personal messages must adhere to the guidelines in this policy and must not breach any of the CCG's other policies or procedures
- Personal emails should be stored in a folder marked 'personal'. It is acknowledged that it is not possible to separate Microsoft Teams messages in this manner. Staff should be aware that personal messages may be viewed by other staff granted access to your Office365 account for legitimate reasons such as absences or IT support

4.11 Misuse of the system

Users must not:

- Use the CCG's email and communication platforms to conduct private or freelance work for the purpose of commercial gain.
- Create, hold, send or forward emails and messages that have obscene, pornographic, sexually or racially offensive, defamatory, harassing or otherwise illegal content. (If you receive such a message you should report it to the IT Service Desk immediately.)
- Create, hold, send or forward emails and messages that contain statements that are untrue, inaccurate, misleading or offensive about any person or CCG.
- Access and use another user's account without permission. If it is necessary to access another user's account then contact the IT Service Desk for details of the necessary procedure. (Users should be aware that access to their email account by authorised individuals may be necessary in periods of absence for business continuity reasons.)
- Send email messages from another member of staff's email account (other than with delegated access) or under a name other than their own. Staff can give delegated access (proxy access) to their account and give permission for colleagues or administrative support to send emails on their behalf.
- Send global emails to ALL staff or to ALL GP practices. There are processes that must be followed for such communications. Contact the Communications Team for advice.
- Send unsolicited emails (spam) to large numbers of users unless it is directly relevant to the recipient's work. (Use staff bulletin/notice boards where appropriate.)
- Send emails to large numbers of users unless the recipients have been blind copied (bcc)[2]. (If the email is not blind copied, individual email addresses will be visible to everyone on the list which may compromise a recipient's confidentiality)
- Send emails to a distribution list comprising members of the public unless the recipients have been blind copied (bcc)[2].

[2] To send a blind copy in Outlook In a message, click on the "Options" tab and in the "Show Fields" group, click Bcc. Place all recipients or the distribution list in the 'BCC:' field that will appear in the message window. The delivered email will suppress the list of other recipients.

- Use blind copying as a matter of course (except in the above circumstances) where its purpose is to withhold from the primary recipient the fact that an email has been copied to a third party. Communication should aim to be transparent and the use of blind copying in this manner an exception rather than the rule.
- Send or forward chain letters or other similar non-work related correspondence.
- Use email for political lobbying.
- Knowingly introduce to the system, or send an email or attachment, containing malicious software, e.g. viruses.
- Forge or attempt to forge email messages, for example, spoofing.

4.12 Reporting Incidents

- Users must report serious incidents of unacceptable use, for example, obscene or racially offensive emails to their line manager or, where this is not possible, to the Deputy SIRO directly. If in doubt, contact the IG Lead for advice.
- All staff are responsible for reporting information incidents and near misses, including breaches of this and any other policy. They should be reported in line with the Incident Reporting Policy.
- Significant Cyber-Security or Data Protection breaches must also be reported to the national bodies via the DSP Toolkit within 72 hours. www.dsptoolkit.nhs.uk Please contact the IG Lead in such circumstances.
- Any instances of suspected fraud should be referred to the Local Counter Fraud Specialist

4.13 Spam and Phishing Emails, messages and calls

- Staff must be aware of and avoid opening unwanted unsolicited emails and messages known as Spam.
- Some unsolicited messages contain malicious web links which are intended to compromise network security and / or steal confidential information by masquerading as legitimate communications. These are known as Phishing.
- Where such emails have be opened inadvertently staff MUST NOT click on any links within the emails.
- Such emails can be forwarded **as an attachment only** to spamreports@nhs.net.
- Where a link in has been clicked in a suspected phishing or spam email, the IT Service Desk must be informed immediately.
- The *Cyber Security Guide* available on the NHSMail website https://portal.nhs.net/Help/policyandguidance contains further advice and guidance on dealing with threats via email.

4.14 Retention and Destruction

The CCG reserves the right to retain email as required to meet its legal obligations.

For NHSMail – staff data is stored for as long as the account is active. An account will remain active if it has been logged into, had a password change, or sent an email within the last 365 days. Shared mailbox data is stored until deleted, then retention policies maintain data for 180 days.

For Office365 applications such as Teams, SharePoint, etc, data is stored until either the data is specifically deleted or the sites containing the data is deleted. Retention periods maintain deleted data for 180 days (since last edited).

As part of an official investigation, data within the retention period of 180 days (since last edited) can be accessed for the following Office 365 applications (when enabled):

- OneDrive
- SharePoint site collections
- Office 365 groups (including emails to groups, conversation and files transferred in Teams channels conversation and file transfer)
- Teams private (one-to-one) conversation (IM only)
- Recorded Teams conversations available via the application Stream

4.15 Further Information

- Further information about the policy can be obtained from the CCG's Information Governance Lead.
- Questions or problems regarding the use of email, MS Teams or the wider Office 365 system should be directed to the IT Service Desk during opening hours. There is no out of hours or home support.

5 Monitoring effectiveness of the policy/procedural document

- All NHS email is monitored for viruses, malware and spam.
- All email (incoming and outgoing) on NHS systems is logged automatically.
- Monitoring logs are audited periodically.
- Activity Monitoring and Data Loss prevention tools are available to the CCG and will be used to ensure the CCGs compliance with legislation and other obligations
- The use of email is not private. The content of email is not routinely monitored but the CCG reserves the right to access, read, print or delete emails at any time.
- Any monitoring or interception of communications will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018, the UK General Data Protection Regulation, the Human Rights Act 1998 and specific procedures around monitoring and privacy.

6 Review

6.1 Investigating breaches of this policy

The CCG will:

- Investigate breaches of this policy, actual or suspected, in accordance with CCG procedures.
- Where appropriate, invoke the CCG's disciplinary procedure for breaches of this and the Fraud Bribery and Corruption Policy.
- Where appropriate, make a complaint to an individual's employing organisation and co-operate fully into any investigation of that complaint where breaches of this policy are committed by users who are not employees of the CCG (such as staff on secondment to the CCG, Honorary Contract holders and users given access to systems by agreement between the CCG and the user's employing organisation).
- Where appropriate take legal action (that is, criminal or civil proceedings) in respect of this policy.

6.2 Liability

- The CCG will not be liable for any financial or material loss to an individual when using email or Office365 for personal use or when using personal equipment to access work email.

This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed after 12 months and thereafter on a bi-annual basis or when a change in legislation dictates.

7 References and links to other documents

- All staff are expected to comply with this policy as well as the NHS Mail policies and guidance published on the NHS Mail portal, https://portal.nhs.net/Help/policyandguidance
- **In particular the NHSMail Acceptable Use Policies (AUP) which cover the use of NHSMail MS Teams and Office 365 must be adhered to**.
- This policy is based on current law, NHS Information Governance standards and accepted standards of good practice; your duty to handle CCG corporate and person confidential information appropriately arises out of common law, legal obligations, staff employment contracts and professional obligations.[3]
- Any breaches of this policy will be fully investigated in accordance with CCG processes which may result in disciplinary action, referral to the Local Counter Fraud Specialist for further investigation and, if appropriate, your employment or association with the CCG being terminated. It may also bring into question your professional registration and may result in disciplinary, civil or criminal proceedings.
- If there is anything that isn't clear or which you do not understand in this policy you must contact your line manager, in the first instance, or the Information Governance Lead for further information.
- Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time. You will be alerted to this via established CCG communication routes.

8 Equality & Diversity Statement

NHS Sheffield CCG aims to design and implement services, policies and measures that meet the diverse needs of our service population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability. Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

NHS Sheffield CCG embraces the six staff pledges in the NHS Constitution. This policy is consistent with these pledges.

[3] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

9 Disability Confident

NHS Sheffield CCG has been accredited with the Disability Confident Award – level 1. This is in recognition of meeting the commitments regarding employment of disabled people and permits the organisation to use the Disability Confident logo on all of its stationery. The Disability Confident symbol should be added as a footer to all policies / procedural documents.

NHS Sheffield Clinical Commissioning Group

NHS Sheffield CCG Equality Impact Assessment 2016

Equality Impact Assessment

Title of policy or service:	Email Digital Teamworking and Videoconferencing Policy	
Name and role of officer/s completing the assessment:	Gershon Nubour, Information Governance Manager ()	
Date of assessment:	26 January 2021	
Type of EIA completed:	**Initial EIA 'Screening'** ☐ ***or*** **'Full' EIA process** ✓	

1. Outline	
Give a brief summary of your policy or service • Aims • Objectives • Links to other policies, including partners, national or regional	Sets out to staff the appropriate use of email including the transfer of person identifiable information.

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;

- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is justified, eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information
This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

	What key impact have you identified?			For impact identified (either positive an or negative) give details below:	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	x	☐		
Age	☐	x	☐		
Carers	☐	x	☐		
Disability	☐	x	☐		
Sex	☐	x	☐		
Race	☐	x	☐		
Religion or belief	☐	x	☐		
Sexual orientation	☐	x	☐		
Gender reassignment	☐	x	☐		
Pregnancy and maternity	☐	x	☐		
Marriage and civil partnership (only eliminating discrimination)	☐	x	☐		
Other relevant groups	☐	x	☐		
HR Policies only: Part or Fixed term staff	☐	x	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them to onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	**Lead / Reviewing Officer:**	**Information Governance Manager** **Information Governance Group (Sheffield CCG)**	**Date of next Review:**	**January 2023**