North Tyneside
Clinical Commissioning Group

Information Governance	IG07: Internet/Intranet Acceptable Use Policy

Version Number	Date Issued	Review Date
V5.1	January 2021	November 2022

Prepared By:	Senior Governance Manager, NECS
Consultation Process:	CCG Head of Governance Quality and Safety Committee

Policy Adopted From:	Internet / Intranet Acceptable Use Policy (4.1)
Approval Given By:	Quality and Safety Committee 5 January 2021 TBC

DOCUMENT HISTORY

Version	Date	Significant Changes
V1	March 2014	None
V2	September 2014	None
V3	January 17	None
V4.1	July 2018	Update in line with GDPR and Data Protection Act 2018
V5	April 2020	Review. Minor amendments made throughout the policy.
V5.1	December 2020	Section 2.1 added relating to 'Prevent'

EQUALITY IMPACT ASSESSMENT

Date	Issues
August 2020	No issues identified.

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3 year period.

ACCESSIBLE INFORMATION STANDARDS

If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact necsu.comms@nhs.net

Contents

1. Introduction

1.1 E-mail, the intranet and the internet are used widely by staff within the CCG to support them in undertaking their duties. It is important that staff use e-mail and the Internet professionally and efficiently to maximise benefits to the organisation. The CCG is legally obliged to ensure that all staff are protected against viewing or accessing inappropriate materials. It is therefore mandatory that employees adhere to this Policy when communicating by e-mail or using the Internet. Failure to follow this Policy may lead to disciplinary action being taken against the user.

1.2 Policy Statement

1.2.1 The purpose of this document is to present a policy for the acceptable use of the intranet, the internet and email. This sets out the expectations of the CCG for the proper use of its email systems and compliments other Information Governance policies. Its aim is to ensure the appropriate and effective use of the internet and email by:

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

1.2.2 This policy is applicable to all employees, agents and contractors working for, or supplying services to the organisation. However, it is recognised that primary care practitioners are also part of the organisations and as such this policy is offered for use by them to adapt to their own practices and organisations as appropriate.

2. Definitions

2.1 **Encryption** is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.

2.2 **GDPR** is the General Data Protection Regulations - a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) and part of the Data Protection Act 2018.

2.2 **NHS Mail** is the e-mail and directory service specifically designed to meet the needs of NHS staff which allows e-mail to be sent in an encrypted form. It is the only Department of Health (DoH) approved NHS e-mail service for securely exchanging personal data between NHS approved organisations but needs to be used by both sender and recipient in order to be secure.

2.3 **Personal information** is factual information or expressions of opinion which relate to an individual who can be identified from that information or in conjunction with any other information coming into possession of the information holder. This also includes information gleaned from a professional opinion, which may rely on other information obtained.

2.4 **Proxy Server/Setting** is a software agent that performs a function or operation on behalf of another application or system while hiding the details involved.

2.5 **Pseudonymisation** is the process of enhancing privacy by replacing most identifying personal data fields within a data record by one or more artificial identifiers, or pseudonyms (e.g. replacing names with codes or numbers.

2.6 **Streaming media** is any kind of Internet content that is continuously transmitted such as radio broadcasts, video e.g. YouTube, Google Video, Internet radio

2.7 **Spam** is unsolicited commercial email, the electronic equivalent of the junk mail that comes through your letterbox.

2.8 **Subject Access Request** is a request made by or on behalf of an individual for their held personal data which he or she is entitled to ask for under Data Protection Legislation 2018.

2.9 **Subject Rights Request** is a request made by or on behalf of an individual for their personal data to be corrected, erased, ported to another organisation, or to have the way it is processed altered as per the rights of the data subject under Data Protection Legislation 2018.

2.10 Defamation & libel

2.10.1 <u>What is defamation & libel?</u>

A published (spoken or written) statement or series or statements that affects the reputation of a person (a person can be an individual or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person(s) affected may have legal redress rights.

2.11 Harassment

2.11.1 What is harassment?

Harassment can be verbal; non-verbal; physical; or other. Harassment is defined as any conduct which is:

- Unwanted by the recipient
- Is considered objectionable by the recipient
- Causes humiliation, offence and distress (or other detrimental effect)
- Any of the above witnessed by a third party

a) **Verbal Harassment** unwelcome remarks, suggestions and propositions, malicious gossip, jokes and banter, offensive language.

b) **Non-Verbal Harassment** offensive literature or pictures, graffiti and computer imagery, isolation or non-co-operation and exclusion from social activities.

c) **Physical Harassment** ranging from touching to serious assault, gestures, intimidation and aggressive behaviour.

d) **Unwanted conduct** relating to a protected characteristic which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual.

Further detail can be found in the Harassment and Bullying at Work Policy, HR12.

2.12 Pornography

2.12.1 What is pornography?

The CCG defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The CCG will not tolerate its facilities being used to view, share, create, download, or store this type of material and considers such behaviour to constitute a serious disciplinary offence.

2.13 Copyright

2.13.1 What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be any data asset such as a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law

2.13.2 What you must not do

- Alter any software programs, graphics etc. without the express permission of the owner.
- Claim someone else's work is your own.
- Send copyrighted material by Internet without the permission of the owner. This is considered copying.

2.14 Prevent

2.1.4.1 What is Prevent?

The aim of the Prevent strategy is to reduce the threat to the UK from terrorism by stopping people becoming terrorists or supporting terrorism. In the Act this has simply been expressed as the need to "prevent people from being drawn into terrorism". The 2011 Prevent strategy has three specific strategic objectives:

- respond to the ideological challenge of terrorism and the threat we face from those who promote it
- prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
- work with sectors and institutions where there are risks of radicalisation that we need to address.

3. Access To and Use of Email Systems

3.1 E-mail is an important means of communicating quickly and easily to support the business needs of the organisation. However e-mail can be used inappropriately, either deliberately or otherwise. Remember that any e-mail, sent or received, may have to be disclosed in litigation, as part of an internal or external investigation, following a Subject Access Request, or Subject Rights Request regarding personal data under GDPR, or following a request under the Freedom of Information Act.

3.1.2 The provision of connection to electronic mail will be granted upon receipt of an authorised request being made via the ICT Service desk website provided by the Commissioning Support Unit (CSU). All users must have their requests for access authorised by the nominated access lead/s in the CCG.

3.1.3 Use of the electronic mail system(s) will be logged and monitored and where the facility has been abused, disconnection will follow. If evidence exists to show use of the system contrary to CCG policy or UK law (including the Privacy and Electronic Communications Regulations (PECR), this will lead to disciplinary action.

3.1.4 Electronic mail should primarily be used for CCG business. Personal use is discouraged however occasional personal use will be permitted as long as this time is reasonable and does not infringe on work time or is considered to be inappropriate use. The CCG recognises that transactions made via NHS Discounts are personal, therefore must be made in line with this policy, however the CCG acknowledges that such transactions require the use of an NHS Mail account in order to perform a transaction with NHS Discounts.

3.1.5 The CCG provides electronic mail as a means of communication in respect of CCG business. Whilst the CCG is aware that from time to time e-mail is used for non-work purposes, all staff are reminded that it is not designed for these purposes. As a result e-mail must not be used to send any material, which could be considered offensive, pornographic or illicit. Also users should not use e-mail as a means of circulating humour, gossip and chain emails. The CCG reserves the right to audit emails if abuse is suspected.

3.1.6 Electronic mail must not be used for personal financial gain or other secondary employment.

3.1.7 Electronic mail must not be used for any purpose which would contravene any existing UK law, any stated policy of the CCG, or which might be considered generally offensive.

3.1.8 All electronic mail users are reminded that the laws covering copyright, data protection and libel apply to all electronic mail messages.

3.1.9 Electronic mail users may not attempt to make any alterations to the configuration of their electronic mail software but may customise their own electronic mail view and grant proxy rights to other staff.

3.1.10 All electronic mail users are reminded that some electronic mail is not a secure medium and as such confidential or patient related information must not be sent unless this is via NHSmail. The NHSmail service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services. Further guidance is available at Appendix A.

3.1.11 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, users can be given proxy access to another user's email account where this has been authorised, for example when a user is off sick or on leave and access is necessary for the proper functioning of the business).

3.1.12 Users must log off the network or lock their terminal whenever they leave their desk. This can be done by pressing and holding the Windows button and the 'L' key on the keyboard.

3.1.13 When accessing email systems via a portable device, such as a smart phone this device must be locked using a Personal Identification number (PIN) or finger print (if available).

3.1.14 Email is a communication tool and not a records management system. Where the content of email or attachments forms part of a record it is the responsibility of the user to ensure it is added to, and becomes part of, that record whether held in hard copy or electronic format.

3.1.15 Email users must remember that under Data Protection Legislation 2018 any emails about or referring to a data subject can be requested by them as a Subject Access Request.

3.1.16 Users must not:

- Automatically forward email from their email account or send confidential or sensitive information to non NHS.net email accounts. Examples of non-NHS email accounts include hotmail, yahoo, AOL, and email services provided by internet service providers

- Create, hold, send or forward emails that have obscene, pornographic, sexual or racially offensive, defamatory, harassing or otherwise illegal content. (If you receive such a message you should report it to the ICT help desk immediately)

- Create, hold, send or forward emails that contain statements that are untrue, inaccurate, misleading or offensive about any person or organisation

- Access and use another's email account without permission. (If it is necessary to access another user's account then contact the ICT support desk for details of the necessary procedure)

- Send email messages from another member of staff's email account or under a name other than your own. (Secretaries may send emails in their own name on behalf of their manager if instructed to do so)

- Use email for political lobbying

- Knowingly introduce to the system or send an email or attachment containing malicious software for example viruses

- Forge or attempt to forge email messages, for example spoofing (forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source).

- Use instant messaging services for example Microsoft Messenger. For guidance on the use of instant messaging in an emergency please refer to the CCG's Social Media and Instant Messaging Policy

- Send or forward chain letters or other similar non work related correspondence

- Send unsolicited emails (spam) to a large number of users unless it is directly relevant to the recipients work (use newsletters/intranet where appropriate)

- Send or forward large messages or attachments (examples of large attachments include photographs, large documents, electronic greetings and flyers). The sending and storage of large attachments can cause the network to slow down or crash and can seriously affect the CCG's capacity to store files

- Open or click on any attachments within an email which do not appear to be from a genuine, reliable source. If in doubt contact the ICT service desk for advice

3.1.17 Take any documentation for future reference when changing roles or leaving the organisation unless agreement of the line manager has been sought. Email is provided primarily for business purposes, therefore emails are the property of the CCG, not the individual. Where agreement has been given to take emails for future reference, this must be done so under the supervision of the line manager.

3.1.18 Guidance on the use of email to accompany this email policy is at appendix A.

3.2 Using the Internet

3.2.1 Acceptable Internet Usage

3.2.1.1 Access to the Internet is provided primarily for work-related purposes, including research related to studies approved by the CCG and professional development and training.

3.2.1.2 The provision of connection to electronic mail will be granted upon receipt of an authorised request being made via the ICT Service desk website provided by the CSU. All users must have their requests for access authorised by the nominated access lead/s in the CCG.

3.3 Unacceptable Internet Usage

3.3.1 No member of staff is permitted to access; display or download from Internet sites that hold offensive material; to do so is considered to be a serious breach of security and may result in dismissal. Examples of unacceptable use are as follows;

- Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

- Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.

- Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.

- Creating or transmitting "junk-mail" or "spam". This means unsolicited commercial webmail, chain letters or advertisements.

- Using the Internet to conduct private or freelance business for the purpose of commercial gain.

- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware.

- Breach copyright for example by; using someone else's images or written content without permission; or failing to give acknowledgment where permission has been given to reproduce something.

Further guidance on using social networking sites is available from the CCG's Social Media Policy.

The use of forums bulletin boards and newsgroups is permitted however these facilities are only authorised for business purposes. Forums and bulletin boards generate large amounts of email and therefore should only be used selectively.

Staff are not permitted to publish any confidential information on bulletin boards, forums or newsgroups

Staff other than those with documented permission should not download software or programs from any websites without express permission from the CSU ICT department. This applies even if the software/program appears to be from a legitimate website

3.4 Monitoring Compliance

3.4.1 Monitoring Internet Use

3.4.1.1 The CSU ICT Department has implemented a tool which monitors, and in some cases blocks access to specific web sites to users of the network. This software allows logs to be kept showing which staff have accessed which sites. Managing unacceptable use of the Internet will take two forms; standard regular monitoring by the CSU ICT Department, and ad-hoc via issues raised by members of staff.

3.4.2. Regular monitoring

3.4.2.1 On a monthly basis the CSU ICT Department will generate reports from the monitoring tool which will provide information on the following:

- Staff accessing inappropriate categories of websites (even if these sites have been blocked),
- Staff accessing non-work related sites excessively in work time,
- Staff trying to access the Internet anonymously e.g. through attempting to bypass existing security settings and remote proxies,
- Where unusual activity is detected the CSU ICT Department will investigate further in line with the Monitoring of Internet and E-mail Procedure.

3.4.3 Ad hoc reporting

3.4.3.1 In addition to regular reports, specific issues in Internet or email usage may be highlighted by other means for example, a user's line manager. These would be reported to the Head of Governance. In such a case, no information would be provided to the line manager, unless a clear breach of policy had been identified and then in line with the investigation process detailed below. The line manager would be informed if the reports indicated that no specific issue had been highlighted by the monitoring system. Requests for investigation can only by authorised by the Senior Information Risk Owner (SIRO).

3.4.4 E-mail Monitoring

3.4.4.1 The e-mail system is provided for CCG business purposes. All e-mail messages are business documents of the CCG and may be accessed without the employee's permission for legitimate purposes e.g. investigation of potential breaches of this policy or the Security Policy or legislative reason such as Freedom of Information or Subject Access Requests. This will be carried out by a limited number of identified staff with appropriate regard for the confidentiality of the content in line with the CSU's Monitoring of Internet and E-mail Procedure. Some CCG staff are GPs and will utilise NHS mail for both CCG and GP business. This policy covers only the work carried out on behalf of the CCG.

4. Breach of this Policy

4.1 Any identified breach of this policy may be deemed to be misconduct and as such may constitute grounds for disciplinary action under the CCG's Disciplinary Policy.

4.2 Following investigation and due process, possible disciplinary action taken in relation to breaches of this policy includes, but is not limited to:

- Informal Warning
- First Written Warning
- Final Written Warning
- Removal, restriction or monitoring of internet and email usage

4.3 Certain serious breaches of this policy may be deemed to be Gross Misconduct for which Summary Dismissal, being dismissal without notice is a possible outcome.

5. Duties and Responsibilities

Quality and Safety Committee	The CCG's Governing Body has delegated responsibility to the Quality and Safety Committee for approving CCG policies.
Chief Officer	The Chief Officer as accountable officer has overall responsibility for the strategic direction and operational management, including ensuring that CCG process documents comply with all legal, statutory and good practice guidance requirements.
Chief Operating Officer	The Chief Operating Officer (as SIRO) will ensure that use of email and the internet will: • comply with corporate branding • be used in a manner to enhance the CCG's ability to engage with stakeholders • comply with statutory and regulatory rules as well as national guidance and best practice They are also responsible for: • generating and formulating this policy • identifying the appropriate process for regular evaluation of the implementation and effectiveness of this policy • identifying the competencies required to implement this policy, and either identifying a training resource or approaching Workforce Learning and Development (Governance Directorate CSU) for assistance
All line managers	All line managers are responsible for ensuring that appropriate processes are complied with when using email and the internet.

All Staff	All staff, including temporary and agency staff, are responsible for: • Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken. • Co-operating with the development and implementation of policies and procedures and as part of their normal duties and responsibilities. • Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly. • Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager. • Undertaking training / attending awareness sessions when provided.
CSU Staff	Whilst working on behalf of the CCG, CSU staff will be expected to comply with all policies, procedures and expected standards of behaviour within the CCG, however they will continue to be governed by all policies and procedures.
Information Asset Owners	Information Asset Owners (IAOs) are responsible for: • Liaising with records management/IG leads to ensure that records management practices are in line with the guidance and protocols on confidentiality. • Ensuring appropriate record audits are undertaken. • Ensuring appropriate information governance /confidentiality clauses are in third party contracts relating to records management such as secondary storage, scanning companies before using the company. • Ensuring appropriate consideration is given to records management within business continuity plans. • Ensuring they obtain appropriate certifications of destruction. Investigate and take relevant action on any potential breaches of this policy supported by other applicable staff in line with existing procedures.

6. Implementation

6.1 This policy will be available to all staff for use in relation to the use of email and the internet.

6.2 All managers are responsible for ensuring that relevant staff within their own departments have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

7. Training Implications

7.1 It has been determined that there are no specific training requirements associated with this policy/procedure however all staff are expected to undertake annual Data Security Awareness training.

8. Documentation

8.1 Other related policy documents.

- Confidentiality and data protection policy
- Information governance and information risk policy
- Information security policy
- Records Management policy and strategy
- Safeguarding children policy
- Safeguarding vulnerable adults policy
- Standards of business conduct and declarations of interest policy
- Equality and diversity policy
- Harassment and bullying policy
- Raising Concerns at Work policy
- Disciplinary Policy
- Social Media and Instant Messaging Policy

8.2 Legislation and statutory requirements

- Equality Act 2010
- Data Protection Act 2018
- Freedom of Information Act 2000
- General Data Protection Regulations 2016
- Human Rights Act 1998
- Employment Rights Act 1998
- Trade Descriptions Act 1968
- Crime & Disorder Act 1998
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Trade Marks Act 1994
- Telecommunications Act 1984
- Obscene Publications Act 1959 & 1964
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000

9. Monitoring, Review and Archiving

9.1 Monitoring

The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

9.2 Review

9.2.1 The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

9.2.2 Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

9.2.3 For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

9.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with the DH Records Management: Code of Practice for Health and Social Care 2016.

10. Equality Analysis

Initial Screening Assessment

As a public body organisation we need to ensure that all our strategies, policies, services and functions, both current and proposed have given proper consideration to equality and diversity, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership, Carers and Health Inequalities).

A screening process can help judge relevance and provides a record of both the process and decisions made.

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Beverley Smith Role: Senior Governance Officer

Title of the service/project or policy:

Internet and Email Acceptable Usage Policy

Is this a:

X	Strategy / Policy		Service Review		Project

If other, please specify:

What are the aim(s) and objectives of the service, project or policy:

This policy sets out the expectations of the CCG for the appropriate and acceptable use of the internet and email. It identifies proper use of email systems and compliments other Information Governance policies. The document sets out the users rights and responsibilities and rules relating to sending, receiving and storing emails whilst considering legal requirements and NHS standards.

Who will the project/service /policy / decision impact?

Consider the actual and potential impacts:

- [x] Staff
- [ ] service users/patients
- [ ] other public sector organisations
- [ ] voluntary / community groups / trade unions
- [ ] others, please specify:

Questions	Yes	No
Could there be an existing or potential impact on any of the protected characteristic groups?		X
Has there been or likely to be any staff/patient/public concerns?		X
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?		X
Could this piece of work affect the workforce or employment practices?		X
Does the piece of work involve or have an impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing equality of opportunity • Fostering good relations		X

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

The policy is based on the previous North Tyneside CCG policy. There is no fundamental change to the content therefore the previous EIA which concluded 'no impact' remains appropriate.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document.

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Beverley Smith	Senior Governance Officer	August 2020

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given

Appendix A

GUIDELINES ON THE MANAGEMENT OF E-MAIL

1 INTRODUCTION

These guidelines are to be used for the management of e-mail within the CCG, in particular, the filing and retention of e-mails and are intended to support the email policy. They provide information on which e-mails should be retained, the available storage options and consideration of the length of time for which messages should be kept.

It is important to remember that while email is an excellent tool for communication it is not designed to meet Records Management or long term storage requirements. However, e-mail has become a primary means of conducting CCG business, being used for everything from sending important documents, agreeing contracts and confirming actions, to conveying personal information (NHSmail only) and messages. It is easy to overlook the fact that many e-mails are business records, required for evidential purposes and should be treated accordingly.

2 E-MAILS AS CCG RECORDS

Because many e-mails have a value as organisation records they require to be managed in accordance with the organisations Records Management Policy and the Records Retention Schedules which specify the periods of time for which different types of information should be kept.

Critically, it should be recognised that ***all*** e-mails sent and received by staff in the course of their employment with the CCG are subject to the same legislation as records in other formats, most notably the Freedom of Information Act (2000) and the Data Protection Act (2018).

Increasingly, as e-mails form a significant part of the knowledge base of the organisation, messages which ***should*** be kept must be properly identified, captured and made accessible to the relevant people.

Any and all data assets should be recorded on the CCG's Information Asset Register in order to understand the content, category, location, and flow of data along with any restrictions and/or legal basis for processing. This is a requirement under the General Data Protection Regulations.

3 WHEN IS AN E-MAIL A RECORD?

Not all e-mails are worthy of being retained; indeed, e-mails take up server space, so there is a cost implication associated with excessive retention, which can also result in greatly increased back-up and recovery times. Keeping e-mail messages for too long may also result in a breach of the Data Protection Act.

To ensure relevant e-mails are captured and managed effectively in record keeping systems, staff need to distinguish between different categories of emails (the flowchart below is designed to assist with this process):

- **Core business records**: these e-mails contain information on core business activities. They may need to be retained for operational or legal reasons and they may need to be referenced by others. Examples of e-mails with a value as core business records can include:
    - E-mail expressing approval of action or decision
    - Direction for important action or decision
    - External business correspondence
    - E-mail which could be used to justify decision making process
    - E-mails which set policy precedents

The retention period for e-mail messages in this category should be in line with the retention periods for an activity in the organisations Records Retention Schedules

- **E-mails containing personal data:** these are e-mails containing information about specific individuals, such as patients and staff and should be sent and received via NHSmail accounts only. ***Such e-mails are covered by the Data Protection Act 2018 and include personal sensitive (or 'special category' data) and personal non-sensitive data.***

- NHSmail encryption - The NHSmail service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services. If users need to exchange information securely outside of the secure email boundary they can do so by using the NHSmail encryption feature. Instruction on how to use this feature is available in the NHS Digital document Encryption Guide for NHSmail Version 2.0, October 2016 or from the national NHSmail helpdesk on 0333 200 1133 or email helpdesk@nhs.net.

- **Reference records:** these are work-related e-mails with a transitory value which may need to be retained only in the short term. Examples include:
    - Records for information – staff on duty, holiday notices etc.
    - Invitations and responses to work-related events
    - Meeting notices and arrangements
    - Copies of reports, minutes etc.
    - Copies of newsletters
    - Cover letters "please find attached" etc.
    - Internal e-mail messages received as c.c.

4 SENDING & RESPONDING TO EMAILS

4.1 Sending

It is important to consider 3 key questions before sending an email:

- **Why** are you emailing
- **What** are you emailing
- **Who** are you emailing

Consideration should be given as to whether or not an email is the most appropriate way of communicating the message. Research has shown that face to face communication is the most effective and written messages are the least effective. If the communication can be done by phone or face to face then there is no need to send an email.

When sending an email you should use action-focused subject lines as follows:

- **Action required** i.e. where you require action e.g. completing a questionnaire
- **For Information** i.e. where no action is required
- **Response required** i.e. where action is required in the form of a response

N.B. Where an action is required ensure that a timescale is included within the subject line. For example; '*Action required: Executive Group paper deadline 20th September'.*

The sending and storing of large attachments can cause the CCG network to slow down or crash and can seriously affect the CCG's capacity to store files.

It is recommended that users do not send or forward large messages or attachments. 5Mb is a suggested limit but good practice is below 1-2Mb. (Examples of large attachments include photographs, large documents, electronic greetings and flyers.)

Users should consider alternative ways of making large work documents available to colleagues such as placing documents on the shared drive or server and emailing a link. Alternatively, use other methods of secure file transfer, for example, FTP.

Users should always check attachments before sending to ensure they are the correct attachment and any personal data has been removed if it is not necessary for the recipient to see it.

4.2 Responding

When an email requires a response you should evaluate it in line with the 2 minute rule i.e. if it takes less than 2 minutes do it. If this is not possible you should consider the following options:

- **Delegate** to another member of your team
- **Diarise** time to action the email
- **Delete** the immediately or once actioned

N.B. Once you have determined the action for the email you should file it for reference, see next section.

Users should always consider whether 'Respond to All' is necessary when there are multiple subjects.

5 SAVING TO THE E-MAIL SYSTEM: PERSONAL FOLDERS

This is the best method when

- E-mail messages form a specific series of record and don't require to be integrated with other records, for example queries, items awaiting action/follow-up etc.

If using this method

- Folders must replicate classification schemes of folders with that of other filing classification structures, for example S:/Drives & H:/Drives.
- Save attachments to a shared network area to avoid breaching storage capacity.
- Use the automatic delete and auto archive features to automate the retention process.

It is also useful to prioritise your folders for easy recall. A useful method is to us the @ sign at the beginning of the folder name to bring it to the top of your list, for example:

- @ ACTIONS
- @ EVENTS
- @ READING

N.B. Set up an actions folder for any items you cannot respond to in the 2 minute rule.

6 SAVING TO SHARED NETWORK AREAS I.E. S:/DRIVES

This is the best method to use if

- It would be beneficial to store the e-mails with related electronic documents
- Shared network areas are well organised with enforced procedures

If using this method

- Save e-mails as TEXT files which can embed attachments
- Integrate e-mails in to the relevant classification scheme

7 PRINTING

Printing should be avoided unless

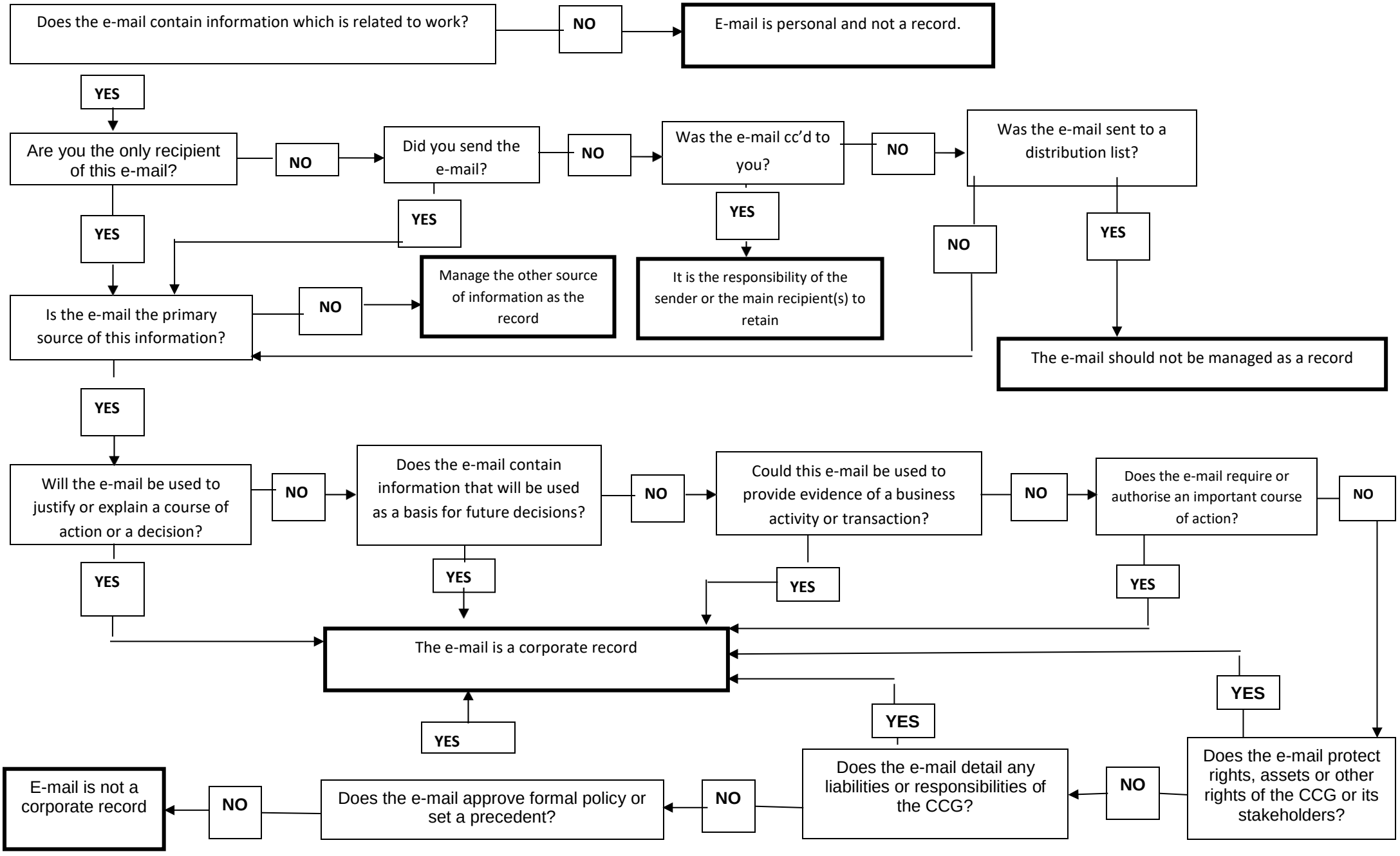
- There is an effective paper file storage system in place
- Working files need all information to be kept together e.g. Project files, meeting papers

If using this method, ensure that the following descriptive information is printed without alteration:

- Sender of the e-mail
- Recipients (including c.c. recipients)
- Date/time of transmission or receipt.

- Avoid printing documents sent for information only and c.c.'d documents
- File printed version in the appropriate file
- Adopt a consistent approach when storing the electronic versions and ensure they are destroyed according to the retention schedules.
- Avoid duplication – if an email is printed, then the electronic version should be deleted.

Appendix B - A flow chart for determining whether e-mails have a value to the organisation



Appendix C

Top tips for managing email

1. When each message is read for the first time, make a decision to save important information to folders then delete the email

2. Use of email for sending the contents of documents in large attachments is discouraged. Documents for general use should be stored in a reliable place such as the network drive.

3. You should clear out your email archive as a matter of routine.

4. You should de-register from mail groups you are no longer making use of as this clogs up the networks

5. You should set up an automatic facility to empty messages from your deleted folder when exiting the email system. This command is accessible through **Tools/Options/Maintenance**

6. Remember email etiquette, which is simply the use of appropriate business-like language. This will avoid confusion on the part of the receiver and ensure that the message is received and understood. It is also important to adhere to the corporate style/branding of the organisation

7. Always use an appropriate 'Subject Line' in your message

8. Always (re)read the email before you send it

9. Use correct grammar, spelling and punctuation as emails should be clear and unambiguous

10. Don't send libellous, obscene, offensive or racist remarks

11. If a message can be relayed verbally via telephone call or face to face then email should be avoided.

12. Delete any emails sent to you in error AND inform the sender of their mistake. Report the error using the SIRMS system if there has been a breach of personal data. Inform the ICO within 72 hours if there has been a serious, wide spread or public breach of personal data.

References
Hare, C. and Mcleod, J. 2006. *How to Manage Records in the e-Environment,* Second edition, London: Routledge