NHS
North Yorkshire
Clinical Commissioning Group

Internet and Email Acceptable Use Policy

February 2021

Authorship:	Senior Information Governance Specialist
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	February 2021
Review Date:	February 2024
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-112
Version Number:	1.1

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as ‘uncontrolled’ and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Senior Information Governance Specialist	First Draft	Information Governance Steering Group (IGSG) - January 2021 Audit Committee – February 2021	
0.2	Senior Information Governance Specialist	Second Draft	Audit Committee – February 2021	
1.0	Senior Information Governance Specialist	Final Approved Version		
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

E-mail 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.

2.0 Purpose

The purpose of this document is to present a policy for the acceptable use of the internet and email. It 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.

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.

3.0 Definitions / Explanation of Terms

3.1 Encryption

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

3.2 GDPR

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.

3.3 NHS Mail

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. NHS Mail is the only email system that should be used by CCG Staff and should be used in line with NHS Mail acceptable use guidance

3.4 Personal Information

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.

3.5 Proxy Server/Setting

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.

3.6 Pseudonymisation

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.

3.7 Streaming Media

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

3.8 Spam

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

3.9 Subject Access Request

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

3.10 Subject Rights Request

Subject Rights Request is a request made by or on behalf of an individual for their personal data to be corrected, erased, transported 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.

3.11 Defamation & Libel

Defamation and libel are 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.

3.12 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, 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.

3.13 Pornography and Offensive websites

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. Sites deemed inappropriate are those with material that is defamatory, pornographic, sexist, racist, on-line gambling, terrorism and/or such sites whose publication is illegal or risks causing offence. Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website the user must immediately inform their line manager or the IT Service Desk.

Where staff need to access any such websites for the purpose of their job they must be able to demonstrate why they are required and ensure that they are appropriately approved to do so. They must also ensure that all measures are taken to prevent unauthorised access to information obtained from these sites.

3.14 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

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.

4.0 Scope of the Policy

The policy applies to NHS North Yorkshire CCG and all its employees and must be followed by all those who work for the organisation, including the Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

It is important that the CCG protects its legitimate business interests and in particular it’s confidential information. Inappropriate use of the CCG internet of email systems including breach of this policy will be regarded as serious misconduct and may result in:

- dismissal;
- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures;
- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and
- legal action being taken against the discloser and/or any other third party.

If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, they must report it immediately to their line manager, the CCG Information Governance Lead and/or to the CCG’s Senior Information Risk Owner (SIRO) or Caldicott Guardian.

The duty of confidentiality is written into employment contracts. Breaches of confidentiality are a serious matter. Everyone in the CCG must be aware of the importance of confidentiality. All staff need to be aware of their responsibilities for safeguarding service user confidentiality and keeping information secure.

It is a disciplinary offence to access records/ information that you have no legitimate reason to view this includes records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

5.0 Duties, Accountabilities and Responsibilities

5.1 Accountable Officer

Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective Information Governance Framework, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2 SIRO

The CCG’s SIRO is responsible for overseeing the implementation of appropriate processes and procedures to ensure that CCG equipment and systems are used appropriately and in accordance with legal requirements.

5.3 Caldicott Guardian

The CCG's Caldicott Guardian is responsible for overseeing and advising on issues of service user confidentiality for the CCG.

5.4 Corporate Services Manager

Has responsibility for the management, development and implementation of policy procedural documents.

5.5 Line Manager

Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality, protecting information and use of CCG equipment and systems. They are also responsible for monitoring compliance with this guideline and highlighting any concerns as set out in this policy, if they are concerned they should contact the SIRO.

5.6 All Staff

All Staff are responsible for ensuring that they adhere to this policy and use CCG equipment and systems appropriately and legally.

All staff are responsible for adhering to the Caldicott principles, Data Protection and Computer Misuse Legislation, and the Confidentiality Code of Conduct.

Staff will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings);

All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first week of employment (as part of their induction into the organisation) and then updated as appropriate in accordance with the Statutory and Mandatory Training Standard and Information Governance Training Needs Analysis.

The CCG must ensure that all contractors and supporting organisations are working to documented contracts or service level agreements that detail their responsibilities in respect of information governance and security, and confidentiality and data protection. This includes the completion of the Data Security and Protection Toolkit to a satisfactory level.

5.7 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this policy.

6.0 Policy Procedural Requirements

6.1 Access to and use of Email Systems

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.

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 their manager.

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 may lead to disciplinary action.

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 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.

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

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.

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

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.

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 C.

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).

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.

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).

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.

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

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).
- 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.

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.

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

6.2 Using the Internet

6.2.1 Acceptable Internet Usage

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.

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 their manager.

6.2.2 Unacceptable Internet Usage

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.

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

7.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of the analysis, this policy does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

NHS North Yorkshire District 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.

8.0 Consultation

This Policy has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

9.0 Training

Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test, this must be completed by new employees within one week of commencement of employment. Further specific training may be required in line with job roles delegated to staff.

10.0 Monitoring Compliance with the Document

10.1.1 Monitoring of Internet Use

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. The management of unacceptable use of the Internet will take two forms; standard regular monitoring by the ICT Department and ad-hoc via issues raised by members of staff.

10.1.2 Monitoring Email Use

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 appropriate staff, identified as and when required, in conjunction with the CCG's SIRO, Caldicott Guardian and/or the Director of Corporate Services with appropriate regard for the confidentiality of the content in line with the 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.

10.1.3 Investigating Inappropriate internet use

Any concerns identified by the CSU IT Dept will be reported to the CCG's SIRO, Caldicott Guardian or Director of Corporate Services, such concerns will include but are not limited to such as 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.

10.1.4 Ad Hoc Monitoring

In addition to the above, 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 Corporate Affairs. 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).

11.0 Arrangements for Review

This policy will be reviewed every three years and in accordance with the following on an as and when required basis:

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;

- new vulnerabilities; and
- changes to organisational infrastructure.

12.0 Dissemination

This policy will be published on the CCG’s internet and will therefore be available to both staff and the public.

Staff will be made aware of the existence of this policy and all subsequent updates via the staff newsletter.

13.0 Associated Documentation

- Information Governance Framework and Strategy
- Data Protection and Confidentiality Policy
- Confidentiality: Code of Conduct
- Mobile Working Policy
- Subject Access Request Policy

14.0 References

This policy was developed in line with the following practices and legislation:

- Data Protection Act 2018;
- Human Rights Act 1998;
- General Data Protection Regulation 2016;
- The Public Interest Disclosure Act 1998;
- The Computer Misuse Act 1990;
- the common law duty of confidentiality;
- National Data Guardian Standards;

15.0 Appendices

Appendix A – Guidelines on the management of emails

Appendix B – Top Tips for managing Emails

Appendix C – Determining an Emails Value to the Organisation

16.0 Appendix A - Guidelines on the Management of E-mail

16.1 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.

16.2 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.

16.3 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.

16.4 Sending and Responding To Emails

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: Governance 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 intranet 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.

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 session.

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

16.5 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.

16.6 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

16.7 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.

Also:

- 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.

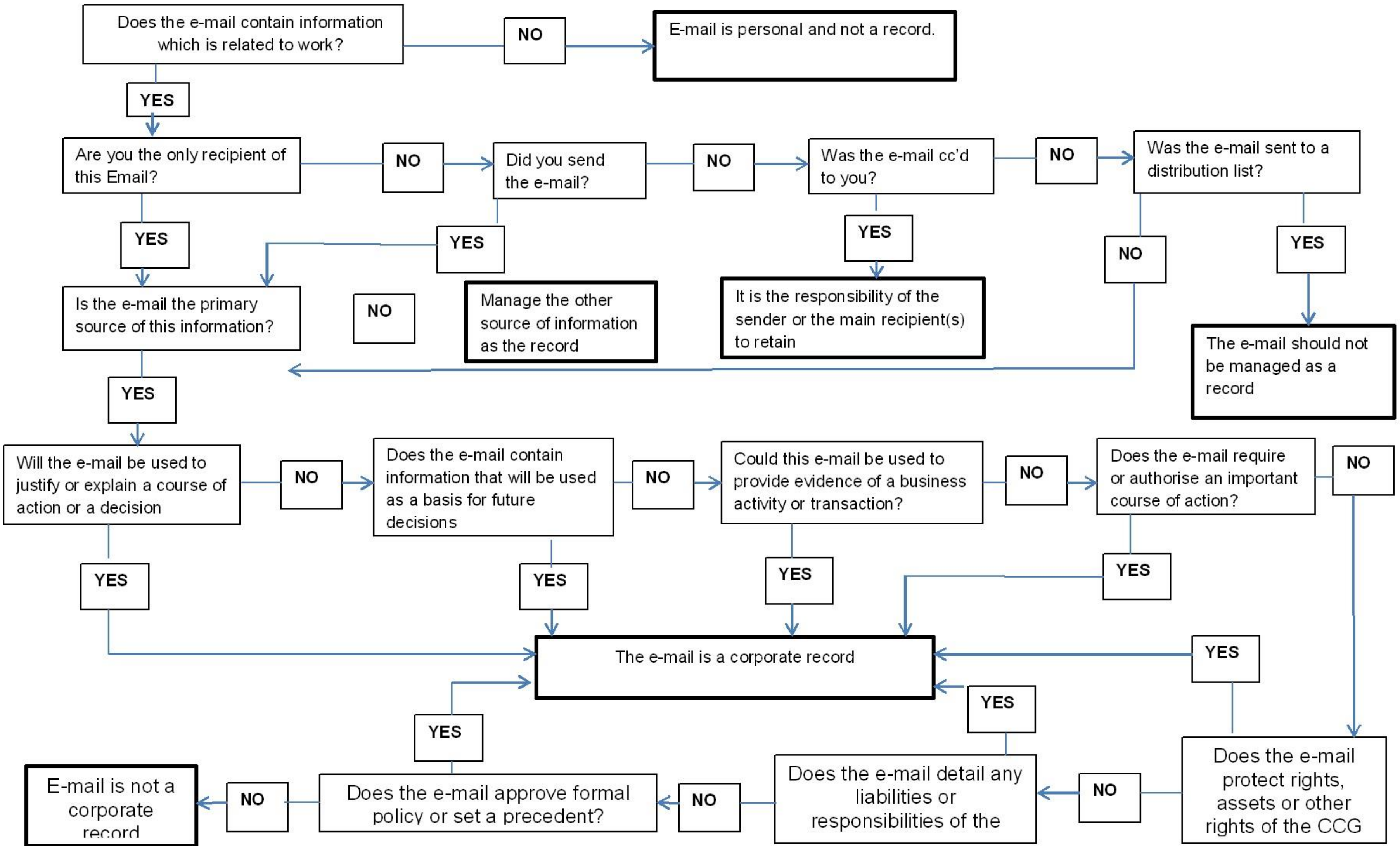
17.0 Appendix B – Top tips for managing email

- When each message is read for the first time, make a decision to save important information to folders then delete the email
- 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 or the intranet
- You should clear out your email archive as a matter of routine.
- You should de-register from mail groups you are no longer making use of as this clogs up the networks
- 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**
- 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
- Always use an appropriate ‘Subject Line’ in your message
- Always (re)read the email before you send it
- Use correct grammar, spelling and punctuation as emails should be clear and unambiguous, which is what grammar, spelling and punctuation rules are for
- Don’t send libellous, obscene, offensive or racist remarks
- If a message can be relayed verbally via telephone call or face to face then email should be avoided, to help avert **death by email!**
- 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

18.0 Appendix C – Determining an Emails Value to the Organisation


Does the e-mail contain information which is related to work?
NO
E-mail is personal and not a record.
YES
Are you the only recipient of this Email?
NO
Did you send the e-mail?
NO
Was the e-mail cc'd to you?
NO
Was the e-mail sent to a distribution list?
YES
YES
YES
NO
YES
Is the e-mail the primary source of this information?
NO
Manage the other source of information as the record
It is the responsibility of the sender or the main recipient(s) to retain
The e-mail should not be managed as a record
YES
Will the e-mail be used to justify or explain a course of action or a decision
NO
Does the e-mail contain information that will be used as a basis for future decisions
NO
Could this e-mail be used to provide evidence of a business activity or transaction?
NO
Does the e-mail require or authorise an important course of action?
NO
YES
YES
YES
YES
The e-mail is a corporate record
YES
YES
YES
E-mail is not a corporate record
NO
Does the e-mail approve formal policy or set a precedent?
NO
Does the e-mail detail any liabilities or responsibilities of the
NO
Does the e-mail protect rights, assets or other rights of the CCG