PLEASE DESTROY ALL PREVIOUS VERSIONS OF THIS DOCUMENT

NHS
Islington
Clinical Commissioning Group

CALENDAR, INTERNET AND E-MAIL POLICY

1	POLICY DRAFTED BY:	NELCSU INFORMATION GOVERNANCE TEAM
2	ACCOUNTABLE DIRECTOR:	DIRECTOR OF QUALITY AND GOVERNANCE
3	APPLIES TO:	ISLINGTON CLINICAL COMMISSIONING GROUP STAFF
4	COMMITTEE & DATE APPROVED:	EMT 7th December 2016
5	VERSION:	1.0
6	RELATED DOCUMENTS:	CONFIDENTIALITY AND DISCLOSURE OF INFORMATION POLICY INFORMATION GOVERNANCE POLICY INFORMATION GOVERNANCE FRAMEWORK AND STRATEGY INFORMATION MANAGEMENT POLICY INFORMATION SECURITY POLICY
7	DATE OF IMPLEMENTATION:	11/01/2017
8	DATE OF NEXT REVIEW:	OCTOBER 2018

DOCUMENT CONTROL

Date	Version	Action	Amendments
07/09/2016	1.0	New policy for Islington CCG in line with policies issued by NELCSU in accordance with SLA	

Contents

1. Summary

Islington Clinical Commissioning Group (CCG) has put this policy in place to ensure staff are fully aware of their responsibilities in relation to the use of:

- Calendars (Electronic)
- Email Services
- Internet Services

The CCG is committed to ensuring that such services are available to support appropriate use of resources, communications and improve efficiency. Compliance with all CCG policies is a condition of employment and a breach of this policy may result in disciplinary action.

2. Scope

This policy covers all aspects of holding, obtaining, recording, using, sharing and disclosing of data/ information or records, when using calendar, email or Internet services, by or on behalf of the CCG.

This includes, but is not limited to; staff employed by the CCG; those engaged in duties for the CCG under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

3. Introduction

The following communication services have been provided to support appropriate use of resources, communications and improve efficiency. In using the services all users must be aware of the requirements to comply with this policy in order to ensure access to these services are safe, secure and lawful. Users must also recognise there is both acceptable and unacceptable use of the email service, and must be aware of their obligations to use these services in an acceptable manner.

3.1. Electronic Calendar Services

The CCG provides its staff with access to electronic calendar services through their NHSmail accounts (forename.surname or forenamesurname@nhs.net) which are described collectively as the calendar services.

3.2. Email Services

The CCG provides its staff with access to NHSmail (forename.surname@nhs.net or forenamesurname@nhs.net) which are described collectively as the email Services.

3.3. Internet Services

The CCG provides its staff with access to the Internet services which access both the NHS Network (N3) and the public Internet which are described collectively as Internet services.

4. Roles and responsibilities

The CCG has identified the following relevant roles and responsibilities within the organisation.

Role	Responsibilities
All Staff	It is the responsibility of all CCG staff to read, understand and adhere to this policy. Any queries relating to the policy can be communicated through line management.
Managers	Managers must ensure staff/users are informed of their responsibilities **prior to granting access to systems**. Managers must inform HR about leavers to ensure accounts are disabled when appropriate.
Third parties	The same responsibilities apply to those working on behalf of the CCG whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of the CCG are **required to sign a third party agreement outlining their duties and obligations**.
CCG Member Practices	This policy should be followed where any member is processing information on behalf of or in relation to the CCG delivery of its function's. However it is recommended that similar policy standards are in place within each member practice to manage its own data and information.
CSU IT Service	The CSU will: • Provide infrastructure to enable the implementation of this policy • Support by providing web usage reports where appropriate

5. Policy Standards

This policy, as part of a suite of supporting Information Governance related policies, sets out the standards that those working for and on behalf of the CCG are expected to adhere to when handling data or information.

5.1. Accountability and Governance

The CCG will put in place suitable controls to:

- Assign responsibilities to oversee the delivery of standards set out in this policy
- Report on compliance against Information Governance to a suitable committee within the CCG
- Ensure that all staff have been made aware of their responsibilities, how to comply with them and have available advice, guidance and training to do so

5.2. Authorised Users

Each user is issued with a network account and password which governs access to calendar, email and Internet services. Users must:

- Manage their password in line with the information security policy (not share their password with anyone else).
- If a user suspects that unauthorised users have discovered or guessed their password, it must be changed immediately and the potential security breach reported to the IT Helpdesk and an Incident form completed.

Where access has been intentionally given to other users, the account holder will remain responsible for any destructive or illegal activity carried out by an unauthorised user to whom access has been given.

5.3. Transfer of Confidential Data/Information

Transfer of NHS Official Sensitive or NHS Official Commercial Data/Information must take place securely in line with the Information Security Policy. This will include:

- Personal Confidential Data
- Commercially sensitive data

Such data should be transferred securely in line with the Information Security Policy and supporting guidance which should have suitable protection is in place, unless covered in the authorised insecure transfers, which must constitute one of the following controls:

- Emailing Internally (not outside the network)
- Use of NHSmail (nhs.net) the NHS internal mail system
- Use of NHS Secure File Transfer (need NHS Mail) or other IT approved Secure File Transfer Protocol (FTP) to a minimum of AES 256 Bit encryption
- Encryption to a minimum of AES 256 Bit encryption of files within external emails
- **All CCG staff are required to have an nhs.net account** to support the safe transfer of sensitive data

Authorised Insecure Transfers

Certain individuals will request contact to be made by email to an external (insecure) address, for example via the recruitment or complaints processes. Complying with such requests will not be seen as breach of this section of the policy as long as:

- A clear request for a response to be sent by email has been made
- Verification of appropriate access to the information has been established
- Only emails sent to comply with the request can be made without further consent being obtained

If you are ensure about an email that you feel contains Personal Identifiable Information contact the IT Help Desk and your query will be forwarded to a Security Specialist.

Emailing Sensitive and Patient Identifiable Information to non-NHSmail recipients or accounts

The new NHSmail encryption feature now allows secure exchange of sensitive and personal information with users of non-accredited or non-secure email services, for example those ending in .nhs.uk, Hotmail, Gmail and Yahoo. Attachments are automatically encrypted and remain secure.

Users of non-accredited or non-secure email services can communicate securely with NHSmail users. The new NHSmail encryption feature means that health and social care staff now benefit from a secure service which allows them to communicate across organisation boundaries and industry sectors. NHSmail can now be used securely across the entire health and social care community.

Sending Information using the NHSmail encryption service will not be a breach provided the HSCIC guidance on sending information to non –NHSmail accounts is followed and the communication channel is established and agreed by both parties.

For NHS mail users:

If you have a contact that uses a non-accredited or non-secure email service (e.g. ending in .nhs.uk) with whom you need to exchange sensitive information, you will need to set up the communications channel with them first by sending an initial encrypted email that they can open, read and reply to securely.

The link below provides further information from the HSCIC which must be carefully followed. http://systems.hscic.gov.uk/NHSmail/secure

For non-NHS mail users:

In order to send an encrypted email to an NHSmail user, the insecure email must email the NHSmail account first. The NHSmail account can then reply to, or forward their email and it will remain encrypted. You can also include attachments.

When you have received an encrypted email from an NHSmail user, in order to open it, read it and reply you will need to register for an account with the NHSmail encryption provider. Step-by-step instructions can be found using the link below:

http://systems.hscic.gov.uk/NHSmail/secure

Note the following:

- Before you send an encrypted email, talk to the person you are sending it to – make sure that they are expecting the information and are ready to deal with it appropriately.
- Read the senders guidance document http://systems.hscic.gov.uk/NHSmail/secure/senders.pdf
- It is your responsibility to safeguard any sensitive data you receive – if you are receiving the information on behalf of an organisation, you should do so in line with local data protection and information governance policies.
- If you are sending information to a patient, gain consent from them before you communicate with them via NHSmail and do so in line with your local information governance policies.
- Send the recipient the encryption guidance and wait to receive confirmation by email that they have read the guidance. http://systems.hscic.gov.uk/NHSmail/secure/recipients.pdf
- Send an initial encrypted email (test) to establish the recipient details and wait for response.
- Once satisfied information can be exchanged.
- Email delivery to Internet email addresses (e.g. Hotmail.com) can be unreliable. Sometimes messages are silently lost or sometimes a delivery notification is returned even if the message has not been received by the recipient. Where delivery assurance is required please ask the sender to reply to you confirming receipt.

This link provides further guidance from the HSCIC: http://systems.hscic.gov.uk/NHSmail/secure

5.4. Cloud based services

The CCG recognises the emergence of cloud based providers that deliver calendar, email and Internet based services such as DropBox™, GoogleDrive™ and Evernote®. Such services will

only be used to process NHS Confidential or NHS Restricted information where a contract is in place with the service provider as outlined in the support services section below.

They may be used as a secondary storage medium for non-confidential data so long as it complies with the Information Management and Information Security Policies in particular:

- No original documents are stored without first being saved to secure contracted services such as the network
- Users understand the implications of using such services and without contractual controls have no recourse should data be lost or unavailable for any period of time.

5.5. Computer Virus Protection

It is essential in order to maintain the security and integrity of systems that all files on the users' system from email, disk or other sources are scanned by up to date, reputable anti-virus software. This should be installed and updated on every PC and Laptop.

Where users are made aware of infection on their system they must not send further emails until the IT Help Desk provide confirmation you can proceed to send emails.

Staff will be informed of suspect emails where there is possible risk of infection to their system. Users should not open such emails or any unexpected attachments to messages.

5.6. Software Downloads

Users should not download or distribute any software of any sort, including from the emails or internet unless authorised to do so by IT. See information security policy for more details.

5.7. Financial Transactions

Users using the CCG Internet Service to conduct any personal financial transaction do so at their own risk. The CCG is not liable for any personal financial transactions that are undertaken by staff whilst using the CCG's Internet Service. Users should exercise caution when disclosing any personal, financial or payment card details over the Internet.

5.8. Legal Requirements

There are a number of legal requirements that need to be considered when handling information on calendar, email and Internet services. These include NHS information governance: legal and professional obligations and the following highlighted below:

Legislation	Summary
Data Protection Act 1998	Must ensure the collection, storage or transmission of personal or sensitive personal data is lawful and secure.

Freedom of Information Act 2000	Under the Freedom of Information Act 2000, information including electronic content held by the CCG may need to be disclosed publicly as the Act gives a 'general right of public access to all types of 'recorded' information held by public authorities'. This would include information held in calendars, email and on internet based services.

5.9. Personal Use

The calendar, email and Internet services are provided for business purposes however the CCG recognise the need for individuals to have to carry out some personal tasks at work, e.g. for Internet banking or travel booking etc. You must ensure that your personal use:

- Does not interfere with the performance of your duties;
- Does not take priority over your work responsibilities;
- Does not cause unwarranted expense or liability to be incurred by the CCG;
- Does not have a negative impact on the CCG in any way;
- Is lawful and complies with this policy;
- Is agreed with a line manager first
- Be during unpaid breaks/lunches

The CCG reserves the right to implement an allocation of personal Internet usage where deemed appropriate and to remove the right to use email services for personal use at any time, provided this is effectively communicated in writing to users.

The CCG will not be held liable for any financial or material loss to an individual user in accessing the Internet for personal use

5.10. Inappropriate or Unacceptable Use

Staff must not engage in any activity that may be deemed 'unacceptable', 'offensive' and/or 'unlawful' activities using calendar, email or Internet services. All complaints will be investigated and may result in disciplinary action and it should be noted:

- Violations can result in disciplinary action, criminal charges or both.
- Ignorance is no excuse.
- Users cannot be exempt from the law because they are employees of the CCG and were 'just playing around'.

Unacceptable use may be defined as one or more of the following:

- Creating, downloading and storing or displaying (other than authorised and lawful health care work or research) any obscene or indecent images, data or material or any data capable of being resolved into obscene or indecent images or materials;
- Creating, downloading or storing or displaying (other than authorised and lawful health care work or research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material;
- Creating, downloading, transmitting or displaying material which is designed or intended to annoy, harass, bully, inconvenience or cause needless anxiety to others;

- Downloading, installing and using unauthorised and unlicensed software or routines for purposes such as, but not limited to: streamlining video, audio or gaming;
- Creating or transmitting 'junk mail' or 'spam'. This includes unsolicited commercial webmail, chain letters or advertisements;
- Using the Internet Service to conduct private or freelance business for the purpose of commercial gain; and
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other users' data, computer installation or network.

Where there is disagreement about any activity being investigated as being unacceptable, the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet will be decided by the CCG's Senior Information Risk Owner.

Harassment

Users must be civil and should not send rude, offensive or harassing emails. Any users found sending such emails will be advised to stop sending them immediately and future use will be monitored. Users who feel they are becoming a victim of harassment should report it using relevant CCG Policy. If a user feels they are in danger then they should talk to their manager or the Human Resources department urgently.

Commercial Use

The following commercial uses are expressly prohibited:

- Advertising or promoting of personal business (es).
- Solicitation to buy or sell goods or services for commercial profit.
- Staff will be able to purchase goods for a personal use however such transactions carried out via Internet services are done so at their own risk.

Copyright Infringement

Users must avoid copyright infringement. (See Definitions Section) Any copying and distribution without permission, including electronic copying is prohibited.

Unauthorised Access

Users must never try to bypass login procedures on any computer system or otherwise gain access where they are not allowed or authorised. This is not acceptable under any circumstances and can result in disciplinary action. This may be in breach of the Computer Misuse Act 1990.

Unintentional Access to Obscene/Illegal/Offensive Material

Any User accessing any site considered to be obscene or illegal or offensive in any way must logout of the site immediately. The user must then inform their Line Manager that they have accessed the site and detail how such access occurred.

6. Calendar Policy Standards

The following principles will apply to electronic calendars:

- All calendars will be set to open by standard to all members and staff within the CCG
- The CCG may choose to make calendars available to outside organisations

- Personal appointments should be marked as private to prevent other users from accessing any included details

7. Email Policy Standards

The CCG will expect all members and staff to follow the principles outlined in the Email Standards appendix and underpinned by the expected standards below:

- Emails should not have any content that is deemed libellous, pornographic, sexually or racially offensive, or otherwise illegal.
- Users will not send emails to large number of people (greater than 10 recipients) unless they are convinced there is a business requirement for each recipient to receive such email.
- Sending unsolicited mail to many users ('spamming') is wasteful of user time and can disrupt the service for other users, as such should not be done.
- Use of 'high priority' messages should only be made when a message is genuinely of high priority and requires quick response.
- Each authorised user must undertake regular and efficient housekeeping of their account(s), to maintain optimum functioning of email servers. A limitation of mailbox sizes will be placed at 1GB after which users will be unable to send further emails.
- An individual user's email mailbox should not be used to store records unless it is a 'generic' transferable shared email mailbox where designed and structured to be used for this purpose.
- Staff should not routinely ask for Read Receipts, unless necessary, to emails as these slow system performance down.
- Subject headings should relate to the contents of their email, and where possible include the purpose, i.e. for action, for information etc.
- Staff must follow any guidance issued by the CCG on 'Managing Your Mailbox' to ensure efficient use.
- Users must also be aware that the CCG has the right to monitor the content of all emails sent and received.
- When receiving email attachments from an unknown originator, users must exercise caution in opening such attachments due to the risks of viruses and other harmful code.
- When receiving so-called spam emails, users should not select the 'Unsubscribe' feature of the spam emails, as confirming the email address is real will encourage additional spam emails.
- Users should exercise caution when receiving emails from what may appear to be a reputable organisation requesting any personal or financial details. Where users receive such apparent genuine requests, strong consideration should be given to validating the authenticity of the request by other means, for example by telephone, before providing any such sensitive information.
- Care should be taken by staff when emails come from apparently legitimate sources either seeking details of staff or the organisation for which they work. There have been, and continue to be, cases of "scam" emails purporting to be from legitimate organisations but which either contain malware or are attempts at fraud by "phishing" or other methods. Any suspicious e-mails of this nature are to be reported to ICT. Updates on known issues of this nature will be communicated via the Intranet.

7.1. Efficient Email Usage

All messages, using email should be concise and directed only to interested individuals or those who need to know. Large documents (10mb+) should not be transferred via email. Where possible please provide links to a document location rather than attach a file to reduce email size and duplication of documents. Large files up to 1 GB can be transferred within the NHS network using the NHS Secure File Transfer (SFT) service.

7.2. Generic Mailbox

The CCG will use and encourage the generic mailboxes where:

- A team or multiple people may be required to respond to queries and to allow for business continuity
- A mailbox is required to easily store correspondence in relation to multiple matters
- A senior manager takes responsibility of the mailbox
- Access will be enabled on the express authority of the appointed manager
- The mailbox is transferred and may be used as a permanent storage of information maintained by the IT provider
- Access is to be restricted to those necessary to manage the mailbox

7.3. Auto Forwarding Mail

The use of automatically (auto) forwarding emails is discouraged unless adequate controls are put in place to prevent inappropriate disclosure of information. Particular attention should be made to ensure adherence with other sections of this policy when auto forwarding Emails that may contain confidential or restricted data.

7.4. Use of NHSmail

The CCG recognises the benefits of promoting and use of NHSmail in particular to enable the secure, encrypted exchange of information. As such NHSmail will be used by the CCG where such methods are required and appropriate. In addition the CCG will expect commissioned services to use NHSmail or equivalent secure methods of information exchange where necessary.

8. Internet Policy Standards

8.1. Denial of Service

Internet users will not download, distribute or use in any way any software, application or facility that causes or is likely to cause either denial of Services (DoS), the slowing down or crashing of the CCG's systems and/or applications.

8.2. Personal Blogs and Websites (Social Media)

This part of the policy and procedures in it apply to content that you publish on the Internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

The CCG recognise that in your own private time you may wish to publish content on the Internet. If you post any content to the Internet, written, vocal or visual, which identifies, or could identify, you as a member of the CCG or staff and/or you discuss your work or anything related to the CCG or its business, patients, customers or staff, the CCG expects you to:

- At all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment or membership of the CCG, its policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for or is a member of the CCG.
- Review any personal blog or website that you already have and that indicates that you work for or are a member of the CCG, to see if it breaches this policy and report any such breaches to your line manager.
- Ensure when you express any idea or opinion that you add a disclaimer such as "*these are my own personal views and not those of Islington CCG*".

The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

- Revealing confidential information about the CCG in a personal online posting. This might include revealing information relating to patients, clients, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.
- Criticising or embarrassing the CCG, its clients or its staff in a public forum (including any website). You should respect the reputation of the CCG and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance and follow appropriate policies and processes.
- Publishing comments and/or uploading images of premises, events and staff on Social Networking sites (e.g. Facebook, MySpace, and YouTube) without the prior consent of the person referred to or permission from the CCG. Where these comments are deemed to cause offence staff may be subject of disciplinary measures. Participating in this practice, even outside of working hours, is unacceptable.
- Staff must not access, download or distribute material, or participate in any chat room or Internet community whose subject matter is unlawful, objectionable or liable to cause offence.
- Staff using the Internet facilities of the CCG shall identify himself or herself honestly, accurately and completely (including CCG affiliation and function where requested) when participating in chat rooms or newsgroups, or when setting up accounts on outside computer systems.
- Only those employees or officials who are duly authorised to speak to the media, to analysts or in public gatherings on behalf of the CCG may speak/write in the name of the CCG to any newsgroups or chat room.

Staff are reminded that email and Internet communications are forms of publication and inappropriate use may give result in civil liability. Both words and pictures can be held to be defamatory if they represent an untruth, ridicule a person or cause damage to their reputation. A ‘person’ in this context includes an organisation.

Misuse of the Internet or email can result in legal action against the CCG and, in some cases, also the individual user. If you think that something on a blog or a website could give rise to a conflict of

interest, raise concerns about impartiality or confidentiality then this must be removed immediately and reported to your line manager.

Online publications which do not identify the author as a member of the CCG or staff, do not mention the CCG and are purely concerned with personal matters will normally fall outside the scope of this policy.

8.3. Web-browser Settings

Users are not be permitted to change, or interfere with their web browser settings unless authorised by IT.

8.4. Website Restrictions

In order to ensure the integrity, security and availability of network services access to a number of websites is restricted, given only to limited individuals or strictly prohibited. These can be categorised into certain types or content of websites some of which are listed in **Appendix E**. This list is not exhaustive but is baseline guidance that will be updated as required.

For the purpose of this guidance the following categories of access are to be applied:-

Category	Description
Unrestricted	Access available at all times of the day, subject to such access not adversely affecting work performance
Restricted	Access is only allowed where there is a work related requirement to do so.
Limited Use	Access is allowed for up to 1 hour within one given 24 hour period, subject to line manager agreement and local working practices
Prohibited	No access is allowed at any time of the day, due to the nature of the content, or risk of harm to network.

Some job roles will require access to restricted or limited use sites in order to carry out a specific job role. Such requests will only be granted to that individual, whilst they carry out that specific job. These and any other requests to access restricted sites must be made to the IT Help Desk, by a service manager, with an appropriate rationale for providing access including:

- Business Purpose for Access
- The implications for not being granted access
- Time period access would be required
- Details of the staff requiring access

The IT Help Desk reserves the right to refuse or defer access pending review by the CSU IG team, CCG IG Lead or Senior Information Risk Owner.

9. Training

All staff should access suitable training when using calendar, email or Internet services. Training is available from:

Calendar and Email	Microsoft Training NHSmail Training
Secure exchange of information	Information Governance Training Tool

10. Relationship with Service Providers

As a commissioner of clinical and support services the CCG will ensure that any organisations from which it buy's services meets expected information governance standards.

10.1. Clinical Services

All clinical services commissioned by or on behalf of the CCG will be required to have a suitable policy in place for the secure exchange of data/information. The CCG will expect that commissioned clinical services use NHSmail or equivalent secure communication methods.

Services will need to maintain access to the NHS Network (N3) where deemed appropriate to deliver the service safely and securely.

10.2. Support services

All support services that process information on behalf of the CCG or provide calendar, email and Internet Services to the CCG will only be authorised to access NHS Confidential or NHS Restricted information once they are contractually bound to:

- Follow policy when working on behalf of the CCG
- Maintain appropriate knowledge and resources to implement the policy requirements
- Report any known incidents or risks in relation to the use or management of information owned by the CCG

11. Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with expected Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as "minimal impact".

12. Dissemination and Implementation

This policy will be made available to all relevant stakeholders via the CCG Internet site and will be disseminated via email.

This policy will be supported by a suite of related policies and resources to support its implementation. This will include access to written and verbal advice, additional guidance and procedures where necessary.

13. Non-conformance with this Policy

Should it not possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the departments Information Asset Owner. Any issues will need to be documented as a risk and either:

a. Accepted and reviewed in line with this policy

b. Accepted with a view to implementing an action plan to reduce the risk

c. Not accepted and the practice stop until such time as the risk can be reduced

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action.

All staff are reminded that this policy covers several aspects of legal compliance that both the organisation and as individuals we are responsible for. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958

Failure to comply with this policy may result in criminal proceedings against the individual.

14. Monitoring and Review

The following monitoring will take place to ensure compliance with this policy

14.1. Internet and Email Monitoring

The CCG will monitor e-mail and Internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail; domain names of web sites visited, duration of visits, and non-business files downloaded from the Internet) at a network level (but covering both personal and business communications).

This monitoring will be used to detect and identify potential misuse. Such monitoring might reveal sensitive personal data about you. For example, if you regularly visit web sites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. **By carrying out such activities using CCG provided facilities you consent to our processing any sensitive personal data about you that may be revealed by such monitoring.**

In certain very limited circumstances we may, subject to compliance with any legal requirements, access e-mail marked PERSONAL. Examples are when we have reasonable suspicion that they may reveal evidence of inappropriate or unlawful activity, including instances where there may be a breach of a contract with the CCG.

The CCG will monitor and record, as a minimum, the following events for use of the Internet Service for each individual user:

- User logon (user, time date);
- User logoff (user, time date);
- Duration times;
- Sites visited (recorded by URL or IP Address);and
- Date and time of such visits; and
- All download requests including file transfers.

All logging, accounting and audit information will be backed-up as appropriate and will be securely archived for a minimum of six months.

14.2. Performance

The policy will be monitored in order to determine:

- Availability and dissemination of policy including in alternative formats (where requested or need has been identified)
- Acceptance and understanding by the intended audience (through training, spot checks, surveys)
- Evidence of non-conformance (recording of incidents or highlighting risks)
- CCG compliance against the Information Governance Toolkit

This policy will be reviewed every 2 years and in accordance with the following on an as and when basis:

- Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risks or following reports of serious incidents;
- Changes to organisation infrastructure.

Appendices

Appendix A. Evaluation protocol

Monitoring requirements 'What in this document do we have to monitor'	Compliance with the law Compliance with the Information Governance Toolkit Incidents related to the breach of this policy
Monitoring Method	Compliance with law will be monitored through audit, work directed by the Information Governance Toolkit and as directed by the SIRO The Information Governance Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the IGT will be audited by the organisation's internal audit function before the annual submission. Incident reporting and management requirements
Monitoring prepared by	The CSU Information Governance Team and the CCG IG Lead for the relevant groups Incident reports will be produced by the nominated investigation officer
Monitoring presented to	Relevant CCG committees or groups with oversight of Information Governance Senior Information Risk Owner Caldicott Guardian (CG)
Frequency of Review	Yearly updates will be provided to the relevant groups, the SIRO and the CG Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system Annual (as a minimum) updates to the Board will be provided. The internal audit report on IGT performance will be provided to the Board or delegated sub-committee. Incident Reports will be reviewed on an annual basis and as directed by the seriousness of the incident

Appendix B. Equality and Equity Impact Assessment

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

	Challenge questions	**Yes/ No**	**What positive or negative impact do you assess there may be?**
1.	Does the proposal affect one group more or less favourably than another on the basis of:	No	
	▪ Race		
	▪ Ethnic origin (including gypsies and travellers, refugees & asylum seekers)		
	▪ Nationality		
	▪ Gender		
	▪ Culture		
	▪ Religion or belief		
	▪ Sexual orientation (including lesbian, gay bisexual and transgender people)		
	▪ Age		
	▪ Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)		
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)	No	
3.	Will the proposal have an impact on social environment? (e.g. social status, employment (whether paid or not), social/family support, stress, income)	No	
4.	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)	No	
5.	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)	No	

An answer of 'Yes' to any of the above question will require the Policy lead to undertake a full Equality & Equity Impact Assessment (EEIA) and to submit the assessment for review when the policy is being approved.

Appendix C. Definitions

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)[1] based on the Cabinet Office definition
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data (PCD)	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
NHSmail	A secure, encrypted system of email within the NHS used for the transfer of personal or confidential information and data. Usually associated with an 'nhs.net' email account.	
Internal Mail	Mail which remains within the CCG. May be used for the transfer of physical documents.	
Intranet	The single worldwide computer network that interconnects other computer networks, on which end-user services, such as World Wide Web sites or data archives, are located, enabling data and other information to be exchanged	

[1] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf, p. 24

Email	A system for sending messages from one individual to another via telecommunications links between computers or terminals.	
Asset	Any information system, computer or programme owned by the organisation	
Internet	A global system connecting computers and computers networks. The computers are owned separately by a range of organisations, government agencies, companies and educational institutes.	
Network	A system of interconnected computers, which allows the exchange of information network connection. An individual's access to the network usually involves password checks and similar security measures.	
Software	Computer programmes sometimes also called applications.	
Virus	An unauthorised piece of computer code attached to a computer programme, which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.	
Anti-Virus	Software designed to detect and protect again Viruses. Anti-virus programmes must be regularly updated in order to remain effective. All NHS computers come with automatically updating anti-virus software as standard.	
Cloud	A model for delivering information technology services in which resources are retrieved from the Internet through web-based tools and applications, rather than a direct connection to a server.	

Appendix D. Email Standards

Area	Details
Emails as records	Emails are a corporate record and as such can be requested under Freedom of Information (or the Data Protection Act as part of personal data) to be viewed. There are minimum retention periods for Emails dependent upon their subject matter (please refer to the Information Management Records Policy
Movers & Leavers	When a member of staff is changing roles or leaving, it is the manager's responsibility to set up a process to manage the receipt of new emails and arrange transfer of retained emails to an appropriate Network folder/drive for retention. All remaining emails will be deleted/
Language	Emails should be considered as an important form of communication, as such the language they are written in, the style and format they are written are all important. Personal references and familiarities should not be used when writing a work related email, e.g., do not include a request for personal information at the start, middle or end of a business email.
Style	You should type in normal font size and colour, capitals should not be used as this is a form of shouting and language should be easy to understand and no slang terminology used.
Target readers	Consideration should be given as to whom is sent a copy of an email i.e. who is CC'd in. CC's should only be sent to people who have either an action to perform with the email or to whom the content of the email will add value, or assist. The purpose for CCing should be identified at the top of the email e.g. • CC A Name, Please action point 4 • CC A.N Other, to assist in discussion re: XXXX
Chain emails	If sending large/chain type emails indicate who is responsible for storing the email and where it will be stored – if the email contains any 'business' decisions, whether clinical, financial, personnel etc then this must be kept securely. Ideally store in a Network folder with minimum destruction year marked eg, emails to be destroyed 2014 etc. This will ensure compliance with the Information Management Policy and also that excessive copies are not being saved. If you receive documentation by email that requires saving, this should be saved in an appropriate folder, on a network drive and not stored as part of your emails.
For your information (FYI) Only	If you wish someone to have the email for information only a better process is to send them a copy of the email chain once the chain is complete with a summary of the emails added e.g.:- Reason for email, actions agreed, completion due date.
Absences (planned)	If you are going off work for more than a day you must put an 'Out of Office message on'. Your out of office message should include an expected date of return if possible, relevant contact people for your areas and any other relevant information. You can also grant a colleague or manager access to your email account so that they can check for any emails on your behalf.
Absences (not planned)	If someone who reports to you goes off unexpectedly you will need to contact the IT Help Desk to ask them to either post an out of office message on the individual's account or, with the individuals permission have mail forwarded to your email account or give you access to their

	email account (dependent upon business need auto forward can be performed with consent to support business continuity). This should be removed upon the individuals return to work. Consideration should be given when emailing a colleague/manager whilst they are absent. Returning to hundreds of emails can be a daunting so thought should be given as to whether a) all emails are necessary and, if they are, can you save a draft email with multi attachments or comments and send one completed email on their return. This is more likely to be read and actioned than multiple emails where the importance can be lost.
Subject matters	All emails should contain a subject. This will assist in the filing and retention of the email.
Background	Emails must not have backgrounds on them unless approved by the communications team.
Signatures	Email signatures should detail the following in line with communications style guidance:- ▪ Your name ▪ Your Job Title ▪ Organisation Name ▪ Your Base location/Team Name ▪ Your contact Number(s) ▪ Your email address For reply emails this signature can be shortened to ▪ Your name ▪ Your Title ▪ Your contact number
Keep it professional	Above all emails should be presented in a professional manner. Emails, in many ways, are a replacement for a letter or memorandum and should be treated in this manner.

Appendix E. Guidance on Restricted Web sites

This list is not exhaustive and needs to be viewed on the basis of it being baseline guidance – unrestricted category sites have not been listed.

Category	Examples of Content	Limited Use	Restricted	Prohibited	Comments
Adult Material	• **Adult Content** -- Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses as clubs, nightclubs, escort services; and sites supporting online purchase of such goods and services.			✔	
	• **Lingerie and Swimsuit** -- Sites that offer images of models in suggestive but not lewd costume, with semi-nudity permitted. Includes classic 'cheese-cake,' calendar, and pinup art and photography. Includes also sites offering lingerie or swimwear for sale.			✔	
	• **Nudity** -- Sites that offer depictions of nude or semi-nude human forms, singly or in groups, not overtly sexual in intent or effect.			✔	
	• **Sex** -- Sites that depict or graphically describe sexual acts or activity, including exhibitionism; also sites offering direct links to such sites.			✔	
	• **Sex Education** -- Sites that offer information about sex and sexuality, with no pornographic intent.	✔			
Banking	Sites providing access to personal banking details	✔			
Drugs	• **Abused Drugs** -- Sites that promote or provide information about the use of prohibited drugs, except marijuana, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse.		✔		
	• **Marijuana** -- Sites that provide information about or promote the cultivation, preparation, or use of marijuana.		✔		
	• **Supplements and Unregulated Compounds** -- Sites that provide information about or promote the sale or use of unregulated chemicals (such as naturally occurring compounds).		✔		
Entertainment	Sites that provide information about or promote motion pictures, non-news radio and television, books, humour, and magazines.		✔		
	MP3 -- Sites that support downloading of MP3 or other sound files or that serve as directories of such sites			✔	Possibly copyright Infringement, system capacity restrictions

Gambling	Sites that provide information about or promote gambling or support online gambling		✔		
Games	Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games. Includes sweepstakes and giveaways.		✔		
	Online Gaming			✔	
Illegal or Questionable	Sites that provide instruction in or promote non-violent crime or unethical or dishonest behaviour or the avoidance of prosecution therefore.			✔	
IT	**File Sharing – sites that allow the** distributing of or providing access to digitally stored information, such as computer programs, multi-media (audio, video), documents, or electronic books			✔	Possibly copyright and licensing infringement, system capacity restrictions
	Hacking – Sites that provide information about or promoting unauthorised access to computers, software or databases		✔		
	Proxy Avoidance – how to bypass proxy servers or gain access in anyway bypassing a proxy server		✔		
	Personal network storage, backup and remote access to other systems		✔		
	Software downloads including freeware and shareware		✔		
	Streaming Media		✔		system capacity restrictions
	Web Hosting		✔		Only for work related activities
Internet Communication	**Social Networking**		✔		Only for work related activities
	Internet Radio & TV		✔		Effects system capacity, Licensing and Copyright issues
	Internet Telephony – other than that provided by IT			✔	
	Pay to surf			✔	
	Web Chat -- Sites that host Web chat services or that support or provide information about chat via HTTP or IRC.		✔		
	Web-based Email -- Sites that host Web-based email other than NHSmail			✔	

Militancy and Extremist	Sites that offer information about or promote or are sponsored by groups advocating anti-government beliefs or action.			✔	
Racism and Hate	Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.			✔	
Shopping		✔			
Sports	Sites that provide information about or promote sports, active games, and recreation.	✔			
Tasteless	Gratuitously offensive or shocking, improper language, humour or behaviour			✔	
Violence	Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore, or injury; or that feature images or descriptions that are grotesque or frightening and of no redeeming value.			✔	
Weapons	Sites that provide information about, promote, or support the sale of weapons and related items.			✔	