

Internet and Email Policy

2019 – 2022

Version:	1.0
Approved by:	Audit and Governance Committees
Date approved:	November 2019
Date of Issue (communicated to staff):	December 2019
Next review date:	November 2022
Document author:	Information Governance Delivery Manager

CONTROL RECORD			
Reference Number N&N IG-004	Version 1.0	Status Final	Author Information Governance Delivery Manager
			Sponsor Senior Information Risk Owner (Chief Finance Officer)
			Team Information Governance
Title	Internet and Email Policy		
Amendments	N/A		
Purpose	To ensure that all staff with the Clinical Commissioning Groups (CCGs) are aware of their responsibilities regarding appropriate access to and use of the Internet and Email and potential consequences of misuse for the CCGs and the local health community.		
Superseded Documents	Nottingham City Internet and Electronic Mail Use Policy – v1.2 Mid Nottingham & South Nottingham CCGs Internet and Email Policy V4.0		
Audience	This policy applies to any person directly employed, contracted or working on behalf of the Clinical Commissioning Groups		
Consulted with	Deputy SIRO, Data Protection Officer and Caldicott Guardian		
Equality Impact Assessment	Completed – November 2019		
Approving Body	Audit & Governance Committees	Date approved	November 2019
Date of Issue	December 2019		
Review Date	November 2022		
<p>This is a controlled document and whilst this policy may be printed, the electronic version available on the CCGs' document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.</p>			

Nottingham and Nottinghamshire CCGs' policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at ncccg.team.communications@nhs.net

Contents

1.	Introduction	4
2.	Purpose.....	4
3.	Scope.....	4
4.	Definitions	5
5.	Roles and Responsibilities.....	7
6.	Access	8
7.	Staff Responsibilities	9
8.	Personal Use	10
9.	Use of Social Media.....	11
10.	Transfer of Personal Confidential Data and Confidential Corporate Information	11
11.	Email Retention and Deletion	12
12.	Protection against Viruses.....	13
13.	Incident Reporting.....	13
14.	Misuse of the Internet and Email Systems	14
15.	Investigation of Suspected Misuse	15
16.	Monitoring of Internet and Email Usage	15
17.	Communication, Monitoring and Review	16
18.	Interaction with other Policies.....	16
19.	References.....	17
20.	Equality and Diversity Statement.....	17
21.	Equality Impact Assessment.....	19

1. Introduction

- 1.1. This policy applies to the Nottingham and Nottinghamshire Clinical Commissioning Groups (NHS Nottingham City CCG, NHS Nottingham West CCG, NHS Nottingham North and East CCG, NHS Rushcliffe CCG, NHS Mansfield and Ashfield CCG and NHS Newark and Sherwood CCG), hereafter referred to as 'the CCGs'.
- 1.2. Many information systems are now electronic in the NHS and the internet and email are essential business tools. CCG staff are required to use them in a competent, responsible, effective and lawful manner.
- 1.3. Information created or stored within the organisation's email system constitutes an organisational record. Emails have the same status as any other form of the organisation's business correspondence or written communication and may be subject to disclosure under Data Protection Legislation or Freedom of Information Act (2000).
- 1.4. NHS mail accounts are owned by NHS Digital on behalf of the Secretary of State for England. Nottinghamshire Health Informatics Service (NHIS) under instruction from the CCGs maintains day-to-day administration responsibilities for NHS mail accounts. NHIS also manages access to the internet under instruction from the CCGs and ensures that both internet and email accounts are managed on a least privileged basis.
- 1.5. Staff are granted access to email and the internet for CCG business use and for work-related educational and research purposes. Access for limited appropriate personal use in their own time is allowed with their line manager's permission. Staff are also permitted to use personal devices to access staff Wi-Fi in their own time.

2. Purpose

- 2.1. The purpose of this policy is to ensure that all CCG staff understand their responsibilities for correctly accessing the internet and understand what the organisation deems to be acceptable use of the email system via the organisation's IT systems, while on CCG premises, working remotely and when acting in representation of the organisation.

3. Scope

- 3.1. This policy applies to all CCG staff*.

**For the purpose of this and all other information governance policies, the term 'CCGs staff' refers to the CCGs employees, appointees, temporary staff,*

contractors/agency staff, consultants, students and other individuals working on behalf of the CCGs.

Failure by any member of CCG staff to adhere to this policy and all appropriate supporting guidance will be considered gross misconduct and may result in disciplinary action.

4. Definitions

Attachment: A file attached to an email message, which can contain malicious software and should be opened with care.

Browser: The CCGs use Microsoft Internet Explorer and Chrome as its standard browsers. NHIS will ensure that the current recommended version is available on all devices that access the internet.

Bandwidth: The overall capacity of a network connection/the amount of data that passes through a network connection over time. The greater the capacity, the more likely that better performance will result.

Data Protection Legislation: The General Data Protection Regulation (GDPR) as implemented and modified by the UK Data Protection Act 2018.

Email system: Any computer software application that allows email - message, image, form, attachment, data - to be communicated from one computing system to another.

Information asset: Any data, information, information system, computer or programme of value to the organisation's business.

Information sharing protocols: Written agreements made within the existing legislative framework between the CCGs and named organisations to allow sharing of personal confidential data for health and social care purposes.

Internet (World Wide Web): A global system connecting computers and computer networks. For the purposes of this document, the term internet will also encompass the organisation's intranet.

Intranet: A private network for communicating and sharing information accessible only to authorised users within an organisation e.g. the CCGs' own intranet site or the NHSnet.

Junk mail: Unsolicited email messages usually of a commercial nature, chain letters or other unsolicited mass-mailings (see also **spam**).

Malicious software/Malware: Software designed to harm a computer or network. Includes but is not limited to:

- **Viruses** - unauthorised computer code attached to a computer programme which secretly copies itself using shared discs or network connections - can destroy information or make a computer inoperable,
- **Trojan horses** - malicious, security-breaking programs disguised as something

benign such as a screen saver or game,

- **Worms** - which launch an application that destroys information on a computer and sends a copy of the virus to everyone in the computer's email address book).
- **Ransomware** - a growing threat in the cyber threat landscape. Usually delivered via phishing emails, which use social engineering techniques (i.e. an email made to look like its sent from a person/name know to the victim or disguised to look like it is from your bank, post office, police etc.) to convince a victim to click a link, download or open an attachment. Once the victim's computer is infected with ransomware, the malicious code will begin to encrypt files on the device (and network), rendering them inaccessible before demanding payment, often in the form of crypto currency such as bitcoin, in return for the ability to unlock that data with an encryption key. Effectively this tactic denies the victim access to their data unless they pay the ransom, or have the ability to restore data from unaffected back-ups.

N3: The national broadband network for the NHS, connecting all NHS locations and 1.3 million employees across England. The N3 network enables the user to access NHS Wide Web (nww) prefixed sites, as well as www.

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 policy 'personal' includes the Data Protection Legislation definition of personal data, but it is adapted to include deceased 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.

This excludes the names of staff, their job role and work location, but does apply to their personal data such as home address, date of birth, financial and HR information.

Personal Data (as defined by Data Protection Legislation): Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Phishing: Sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to defraud the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords, credit/debit card numbers and bank account numbers that the legitimate organisation already has. The website, however, is bogus and set up only to steal the user's information (see also **spoofing**).

Proxy website: A server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

Social media: For the purpose of this and other relevant information governance policies the term social media includes, but is not limited to, websites and applications that enable users to create and share content or to participate in social networking, blogging, tweeting or social engineering.

Spam: Unsolicited email messages, usually of a commercial nature sent to a large number of recipients. Refers also to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

Spoofing: Forgery of an email so that it appears to have been sent by someone other than the sender.

User/authorised user: An individual given access to the CCGs' network to access the internet and email.

Wi-Fi: A mechanism for wirelessly connecting electronic devices through a network access point.

5. Roles and Responsibilities

Term	Definition
Chief Officer	The Chief Officer is responsible for ensuring that the organisation complies with the statutory and good practice requirements governing internet and email use outlined in this policy and is supported by the delegated management responsibilities outlined below.
Senior Information Risk Owner (SIRO)	The SIRO has lead responsibility for the security and confidentiality of the organisation's information, ensuring that information risk is properly identified and managed.
Caldicott Guardian	The Caldicott Guardian is responsible for protecting the confidentiality of patient and service user information processed by the organisation, and enabling appropriate information sharing.
Data Protection Officer	The Data Protection Officer is responsible for advising on and monitoring compliance with any Data Protection issues relating to this policy.

Associate Director of Governance/Head of Information Governance	At an operational level, the information governance agenda is led by the Associate Director of Governance, supported by the Head of Information Governance. They are responsible for the effective management of all aspects of IG, including ensuring that systems and processes are in place to support compliance with this policy. They are also responsible for taking a lead in investigating suspected misuse of the Internet or email system.
Associate Director of Performance & Information	As the CCGs lead for IT, the Associate Director of Performance and Information will be responsible for ensuring that appropriate technical solutions are in place to enable the CCGs to manage email and internet effectively in compliance with legislation and NHS guidance.
All Managers	All managers are responsible for ensuring that their staff receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance and legislation. Managers should refer any specific training needs identified to ensure compliance with this policy to the Head of Information Governance
Staff	All CCG staff must be aware of their individual responsibilities for competent and appropriate use of the organisation's internet and email systems, in accordance with this policy and legislation. Staff must inform their line manager if they do not understand any aspects of this policy and/or require further associated training.
Local Counter Fraud Specialist (LCFS)	The LCFS works with the CCGs to investigate any occurrence or allegation of fraud within the organisation and promote awareness of the NHS Counter Fraud initiative amongst staff and patients.

6. Access

- 6.1. All CCG staff requiring computer access will be allocated a network account, email address and access to the internet, following authorisation by an appropriate senior manager. This allows users to log onto a computer, access their email account and utilise the web browser. These services are not available without a username and password.

- 6.2. Access to the internet through proxy websites or other methods of bypassing security controls or circumventing internet filtering to access content otherwise blocked is **not** permitted.
- 6.3. Members of the public are **not** permitted to access the internet via a computer connected to the organisation's network or through a Wi-Fi connection.
- 6.4. Any user who requires temporary exemption from any part of this policy to access specific information for legitimate work or research purposes is required to obtain written authorisation from their Line Manager and Associate Director of Governance.
- 6.5. Users suspected of breaching of this policy may have their access rights suspended until an investigation and any disciplinary procedures have been completed.
- 6.6. **It is vital that line managers ensure all NHSmail accounts are closed/marked as leavers by NHIS once the staff member has left their department/CCG to ensure Web access is closed.**

Further information on computer access control is available in the CCGs' Information Security Policy.

Further information on NHSmail access control can be found in the NHIS NHS Mail Account Management for Managers guide.

7. Staff Responsibilities

- 7.1. The following should be read in conjunction with the NHS Digital [NHS Mail Acceptable Use Policy](#) and the 'Misuse of the Internet and Email Systems' section below.
- 7.2. Staff using the internet and email must conduct themselves in accordance with their terms and conditions of employment or appointment.
- 7.3. Staff must only use the Web Browsers supplied and maintained by NHIS which are Chrome and Windows Internet Explorer. Staff must not load other browsers or ISP (Internet Service Provider) software, later versions / patches or upgrades from CD-ROM, or from the Internet (including Windows updates), without prior authorisation by NHIS.
- 7.4. Staff who intend to make information available over the internet about the organisation's facilities and services must ensure that they liaise with the CCGs' Communications Team and the Branding and Design Guidelines.
- 7.5. Staff must not continue to use an item of networking software or hardware, following a request from NHIS or a CCG manager to cease doing so on the grounds of causing disruption or risk to the correct functioning of the organisation's information systems.

- 7.6. Internet monitoring software is in use which records, prevents access to or warns users about certain categories of sites. Where a user has a legitimate business need to access a restricted site they should complete the online approval form for Access to Blocked Internet Sites.
- 7.7. It is recognised that in the course of their work or associated research, some staff may have a requirement to access, transmit or receive material that may be defined as offensive, obscene, indecent or similar. Any such requirement should be logged with the Information Governance Team. In most cases, such internet sites will be blocked and will require unblocking using the Approval Form for Access to Blocked Internet Sites. Access to pornographic images is deemed to be misuse.
- 7.8. Where files downloaded it is the staff member's responsibility to obey any licensing terms that may apply.
- 7.9. Staff must obtain appropriate authorisation for any use of Cloud Computing services and should refer to the 'Using the Cloud' Staff Procedure for further information.
- 7.10. Downloading images, MP3 files and streaming video or audio can have a significant impact on the performance of the network and must be restricted to authorised business needs only.
- 7.11. Staff are expected to use the same personal and professional courtesy in emails as they would in any other forms of communication. Email messages are written documents and may be used as such in a court of law. They may also be disclosed to the public as the result of a Freedom of Information request. Therefore, staff are advised to create all email messages with a view to them being public correspondence.
- 7.12. Where email is used to communicate externally, users must not give the impression that their personal comments represent the views of the CCGs unless specifically authorised to do so.
- 7.13. The use of email for critical correspondence should not be relied upon without independent verification of receipt.
- 7.14. Email addresses are traceable and identifiable to the organisation and usually to individuals. Any comments made on external websites should contain an appropriate disclaimer that is recommended by the CCGs' Communications Team.
- 7.15. Staff accessing NHS mail from a non-CCG issued device e.g. personal laptop or mobile phone must only do so by using the web version of NHSmail. Users must also log-in under the standard default setting, which does not allow any attachments to be downloaded or any content to be cached.

8. Personal Use

- 8.1. Access to email and the internet is provided to staff for CCG business-related purposes, but it is accepted that they may be accessed for purposes not directly

relevant to the organisation's business. This should be limited and reasonable use and only take place outside an individual's normal working hours or during authorised rest periods, with line management direction, and where this does not interfere with the normal work duties of the individual or others.

- 8.2. There is no absolute right for staff to use email or internet for personal use. Access to the internet and email that is not for CCG business should only take place where it complies with the organisation's view of appropriate use, as indicated by this policy.
- 8.3. Personal emails should be labelled as personal; staff should be aware that personal emails may be accessed under certain circumstances.
- 8.4. The CCGs will not be liable for any financial or material loss to an individual user when using email for personal use.
- 8.5. The CCGs will not be liable for any financial loss to any external supplier of goods and/or services in the event of an individual user failing to honour any financial obligations contracted to that supplier whilst using the CCGs' email system for personal use.

9. Use of Social Media

- 9.1. Access to social media sites is restricted to staff who have a legitimate reason to be provided with access.
- 9.2. Only authorised staff are allowed to communicate on behalf of the CCGs via social media, and the use of the CCGs' corporate logo or other visible markings or identifications associated with the CCGs is not permitted.
- 9.3. All CCG employees and appointees are reminded of the confidentiality statement included in their contract of employment and all staff are reminded of their duty to comply with all information security requirements in the organisation's suite of information governance policies.
- 9.4. Staff must not disclose any CCG information that is or may be sensitive, confidential and person-identifiable, or subject to a non-disclosure contract or agreement.
- 9.5. Staff should not divulge details of their NHS employer on their personal profile pages. If this information is divulged staff must state that they are tweeting/blogging etc in a personal capacity.

10. Transfer of Personal Confidential Data and Confidential Corporate Information

- 10.1. All transfers of personal confidential data must comply with Data Protection legislation and Caldicott Principles. In particular, they should:

- a) Be an approved lawful data flow agreed by the SIRO and DPO.
 - b) Be notified to the Information Governance Team to record on the Data Flow Mapping register.
 - c) Only be sent on a 'need to know' basis.
 - d) Be supported by a justifiable reason to send the information.
 - e) Be pseudonymised, wherever possible.
 - f) Be sent using adequate security as per local and national guidelines.
- 10.2 The principles of confidentiality and data protection must also be applied to the email transfer of information associated with confidential corporate information.
- 10.3 Individual users are prohibited from using instant messaging services such as, but not limited to, Microsoft Messenger or Yahoo Messenger.
- 10.4 Individual users must NOT send or forward PCD or CCG commercially sensitive data to personal non-work email addresses. Examples include but are not limited to Google/Gmail, Hotmail, Yahoo mail, AOL mail, internet or remote storage areas and email services provided by other ISPs
- 10.5 Agreed information sharing protocols must be in place when regularly sending or forwarding PCD to individuals in other organisations.
- 10.6 PCD or CCG commercially sensitive data should only be exchanged electronically when encrypted to at least the minimum security standards. NHSmail sent to secure domains is automatically encrypted and complies with the pan-government email standard.

Detailed Guidance on how to send secure emails can be found in the Safe Haven Procedure.

11. Email Retention and Deletion

- 11.1. Emails must be retained or deleted in line with CCGs' Records Management Policy which adheres to the Health and Social Care Records Management Code of Practice (2016).
- 11.2. Attachments and emails should be saved to an appropriate directory on the shared network drives. Information must not be saved onto the C:Drive or desktop unless this is on an **encrypted** laptop and access to the network is unavailable.
- 11.3. The email system should not be used as a general repository for records.
- 11.4. Emails and their content may be classed as a corporate record and therefore could be requested under the Freedom of Information Act (2000) and the Data Protection legislation. This applies to all retained emails (including those held in 'deleted

Items' and email folders), regardless of their content, sender, whether they relate to the business of the organisation, service users, members of the public, or have been generated by staff for purposes not directly relevant to the CCGs'.

Further details can be found in the CCGs' Freedom of Information Policy.

12. Protection against Viruses

- 12.1. All computer equipment within the CCGs is virus protected, and incoming messages are virus checked. However, users should report any unusual occurrences relating to the performance of their computer to the IT Service Desk.
- 12.2. Receipt of 'suspicious'¹ emails or email attachments should be reported to the NHSmail IT Service Desk via spamreport@nhs.net using the process detailed in the [Cyber Security Guidance](#). Care should be taken or IT advice should be sought before opening any suspicious or unexpected email attachments or links.
- 12.3. Where a 'suspicious' attachment or link has been clicked on staff are instructed to report this to the NHIS IT helpdesk immediately.
- 12.4. The deliberate introduction of viruses or similarly harmful programs will be considered as an act of gross misconduct and action will be taken in accordance with the CCGs' Disciplinary Policy.

Further guidance on protection against computer viruses is available in the CCGs' Information Security Policy.

13. Incident Reporting

- 13.1. All actual, potential or suspected incidents involving use of email or internet need to be documented in line with the CCGs' Incident Reporting Policy.
- 13.2. Incidents may need to be entered on the Incident reporting module of the Data Security and Protection Toolkit. These will usually be incidents where there is a loss of personal data involving a large amount of individuals or particularly sensitive personal and confidential information has been disclosed without the legal basis to do so or in error. Staff should contact their Line Manager, Data Protection Officer, Caldicott Guardian/SIRO as appropriate when reporting incidents.

¹ See the 'Definitions' section of this document for details on phishing, spam, spoofing, and malicious software and malware.

14. Misuse of the Internet and Email Systems

14.1. Misuse of the internet or email system may make both the user and the CCGs liable under law, or may impede the function of the CCGs' network systems and affect wider network users and the efficient functioning of email.

14.2. All users are responsible for complying with the 'Personal Use' and 'User Responsibilities' sections above and for ensuring that they do not use the CCGs' email and internet system for:

- a) Accessing, composing or transmitting any material considered to be illegal, racist, homophobic, immoral, offensive, obscene, libellous, defamatory, harassing or pornographic (other than for lawful and properly supervised purposes – see section 8.7 above).
- b) Accessing or transmitting pornographic images falling into the following categories:
 - Level 1: Adult images
 - Level 2: Explicit images
 - Level 3: Illegal images

Instances where Level 3 images are involved will be reported to the police.

- c) Transmitting material that incites others to criminal, racist, homophobic or terrorist acts or incites them to contemplate such acts.
- d) Creating or transmitting defamatory material (note that common law and statutes pertaining to libel apply to the use of the internet) regarding the CCGs, CCG business, service-users or staff.
- e) Creating or transmitting material designed to or likely to cause annoyance, inconvenience or needless anxiety to service users, other CCG staff or the general public.
- f) Downloading or distributing 'pirated' software.
- g) Transmitting unsolicited commercial or advertising material to other users, organisations connected to N3 or organisations connected to other networks.
- h) Deliberate corruption or destruction of other users' data or work.
- i) Accessing and using other staff member's email account without their permission or any other deliberate violation of another user's privacy.
- j) Undertaking activities that deny service to other staff members e.g. accessing streaming video for non-work purposes, sending unwarranted global emails or excessively large emails.
- k) Any deliberate attempt to disable, defeat or circumvent the organisations' internet firewall and other security measures in place to protect the network.

- l) Downloading any shareware or freeware without authorisation by NHIS.
 - m) Undertaking activities for personal or commercial financial gain (e.g. sales of personal property, gambling or share dealing) or for political lobbying.
 - n) Forging or attempting to forge email messages (e.g. spoofing).
 - o) Streaming of video or audio for personal use without permission.
- 14.3 If any member of staff has concerns about misuse of the internet or email by a colleague, they should inform their Line Manager and the Associate Director of Governance/Head of Information Governance immediately.

15. Investigation of Suspected Misuse

- 15.1. Any suspected misuse of the internet or email system identified through routine monitoring procedures will initially be attributed to, and be the responsibility of, the associated logged-in user.
- 15.2. Where inappropriate use is suspected from the results of routine monitoring or identified through other incidental events the Associate Director of Governance / Head of Information Governance will inform the relevant user's Line Manager and initiate an investigation, in accordance with the CCGs disciplinary policy.
- 15.3. Where the Assistant Director of Governance / Head of Information Governance has concerns about possible fraud and/ or corruption in relation to suspected internet or email misuse, or is in any doubt whether the misuse constitutes fraud or corruption, both the CCGs' SIRO and the Local Counter Fraud Specialist will be informed. Fraud and/or corruption, if proven, may result in criminal action.
- 15.4. Where an event occurs that may warrant investigation digital evidence used about an individual staff member's activity will be processed in line with the CCGs Information Security Policy.
- 15.5. Where any breach of this policy has been established, appropriate action will be taken in accordance with the CCGs' Disciplinary Policy.

16. Monitoring of Internet and Email Usage

- 16.1. Monitoring records will be maintained by NHIS and audited upon a request from the CCGs, audited periodically and only communicated to those with a valid need to know.
- 16.2. If a user inadvertently accesses a site to which they believe access should be prevented they should immediately inform their Line Manager and the IT Service Desk.

17. Communication, Monitoring and Review

- 17.1. The CCGs' Corporate Governance Team will ensure that the policy is circulated to the policy 'audience' as documented in the control section of this document. Also ensuring that any key changes to the policy are highlighted.
- 17.2. This policy will be monitored by the Information Governance team through the review of incident reports where staff are found to have sent information inappropriately or erroneously. The CCGs will also check staff awareness of phishing emails by sending out a test phishing emails. The results of the exercise will inform staff communications, IG Training and awareness activities and may also result in staff being approached at an individual level to undertake further training.
- 17.3. The Associate Director of Governance/Head of Information Governance is responsible for monitoring the organisations' compliance with the procedural and relevant legislative requirements of this policy, supported by assurances obtained from the Data Security and Protection Toolkit self-assessment submissions and the reports on routine monitoring of the use of the Internet and email system.
- 17.4. This policy is one of the information governance policies underpinning the CCGs' Information Governance Management Framework. The Audit & Governance Committees will therefore seek assurances on the overall implementation of this policy when monitoring compliance with the Information Governance Management Framework.
- 17.5. Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the Document Owner.

18. Interaction with other Policies

- 18.1. This policy should be read in conjunction with relevant sections of the following CCG policies and procedures:
 - Information Governance Management Framework
 - Confidentiality and Data Protection Policy
 - Information Security Policy
 - Network Security Policy
 - Electronic Remote Working Policy
 - Records Management Policy
 - Freedom of Information Policy
 - Disciplinary Procedures
 - Fraud, Bribery and Corruption Policy
 - Confidentiality – requirements of IG Staff Code of Conduct and contract of employment

- Safe Haven Procedure
- NHIS NHS Mail Account Management for Managers guide.
- Using the Cloud – Staff Procedure²

19. References

- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1998
- Health and Safety at Work Act 1974
- Human Rights Act 1998
- Health and Social Care Act 2001
- Regulation of Investigatory Powers Act 2000
- Environmental Information Regulations 2004
- Criminal Justice and Immigration Act 2008
- The NHS Confidentiality Code of Practice (Guidelines on the use and protection of patient information, November 2005)
- RCN Legal advice for RCN members using the internet
- British Standards ISO 27001:2005, ISO 27002:2005
- Health and Social Care Records Management Code of Practice (2016)
- General Data Protection Regulation (GDPR) 2016

20. Equality and Diversity Statement

- 20.1. The Nottingham and Nottinghamshire CCGs pay due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, both as commissioners and as employers.
- 20.2. As a commissioning organisation, we are committed to ensuring our activities do not unlawfully discriminate on the grounds of any of the protected characteristics defined by the Equality Act, which are age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.
- 20.3. We are committed to ensuring that our commissioning activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people

² In development at the time of writing this policy.

experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, roma and travellers.

- 20.4. As employers, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.
- 20.5. To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

21. Equality Impact Assessment

Date of assessment:	November 2019			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age³	No	N/A	N/A	N/A
Disability⁴	Yes	Mechanisms are in place via the Communications and Engagement Team to receive the policy in a range of languages, large print, Braille, audio, electronic and other accessible formats.	No	
Gender reassignment⁵	No	N/A	N/A	
Marriage and civil partnership⁶	No	N/A	N/A	

³ A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

⁴ A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

⁵ The process of transitioning from one gender to another.

Date of assessment:	November 2019			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Pregnancy and maternity⁷	No	N/A	N/A	
Race⁸	No	N/A	N/A	
Religion or belief⁹	No	N/A	N/A	
Sex¹⁰	No	N/A	N/A	
Sexual orientation¹¹	No	N/A	N/A	
Carers¹²	No	N/A	N/A	N/A

⁶ Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

⁷ Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

⁸ Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

⁹ Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

¹⁰ A man or a woman.

¹¹ Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. <https://www.equalityhumanrights.com/en/equality-act/protected-characteristics>

¹² Individuals within the CCGs which may have carer responsibilities.