NHS
Bury
Clinical Commissioning Group

Acceptable Use of IT Policy

Version:	3.0
Ratified by:	NHS Bury CCG Information Governance Steering Group
Date ratified:	July 2021
Name of originator /author (s):	Greater Manchester Shared Services - IT Department; NHS Bury CCG Information Governance Manager
Responsible Committee / individual:	NHS Bury CCG Information Governance Steering Group
Date issued:	October 2021
Review date:	July 2024
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers, and contractors
Completed Equality Analysis:	Yes

Further information regarding this document

Document name	Acceptable Use of IT Policy CCG.GOV.019.3.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	IT Manager; NHS Bury CCG IG Team
This document should be read in conjunction with	Information Governance Framework; Information Governance Policy; Data protection and confidentiality Policy; Information Security Policy; Encryption Policy.
This document has been developed in consultation with	NHS Bury CCG Information Governance Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	CCG Corporate Office (Electronic Versions) CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
1.0	NHS Bury CCG IM&T Steering Group	March 2014
2.0	Updated with IM&T Steering group comments	20th January 2016
2.3 = review	NHS Bury CCG Information Governance Team	October 2021
3.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	July 2021

Acceptable Use of IT Policy

Table of Contents

1. Introduction

1.1. This document describes the responsibilities and provides guidance around the acceptable use of IT hardware software and Information assets of NHS Bury Clinical Commissioning Group (henceforth referred to as the CCG).

1.2. The user responsibilities are designed to protect both the CCG as an organisation and its users by making clear how the IT systems provided should be used.

1.3. All users are required to have sight of this policy and be appropriately authorised by their manager prior to gaining access to the IT systems. All updates to the policy will be communicated to staff through internal CCG communications.

1.4. Non-compliance with the clauses in this document may result in disciplinary action.

1.5. If users require more information to clarify an obligation listed here, they should contact the CCG Information Governance (IG) Lead.

2. Scope

2.1. These user obligations cover all activity on CCG provided IT equipment, networks and data sources including mobile phones.

2.2. The policy covers the following areas for acceptable use:

- Responsibilities and use of IT assets
- Use of e-mail and internet
- Network access (including user accounts and password security)
- Guest Wi-Fi
- Mobile device usage
- Data Storage
- Remote access

2.3. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation’s policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

2.4. For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document.

3. General Principles

3.1. In order to protect users and Bury CCG when using CCG IT equipment for CCG business or personal purposes and to ensure proper, secure conduct of business and operations, it is important that any use of this equipment MUST comply with the following principles:

- it does not break the law
- it does not risk bringing NHS Bury CCG into disrepute or placing it in a position of liability
- it does not violate any provision set out in this or any other policy or contravene the CCGs standards of conduct

- it does not cause damage or disruption to the CCG systems or business.

3.2. All data and information residing on the CCG information systems remains the property of the CCG at all times, unless otherwise stated.

3.3. Users accept that personal use of the CCG information systems is not a right and must be exercised with discretion and moderation. Users further accept the CCG will not accept any liability, in part of whole, for any liability for claims arising out of personal use of the CCG information systems or CCG information.

3.4. The CCG retains the right to:

- monitor the use of its information systems for the purpose of protecting legitimate concerns
- prohibit personal use of information systems without warning or consultation whether collectively, where evidence points to a risk to CCG and/or constituent businesses, or individually where evidence points to a breach of this or any other CCG or NHS policy.

3.5. Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not given explicit access or authorisation.

4. Duties and Responsibilities

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

4.2. Overall responsibility for the Acceptable Use of IT policy lies with the CCG Head of IM &T (correct title to be added) Lead who has delegated responsibility for managing the implementation of the policy and associated procedural documents.

4.3. The CCG Information Governance Lead will provide IG advice and guidance and support CCG management where applicable.

4.4. 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 method (e.g. team brief / team meetings); and intranet

5. Computer Misuse

5.1. All users are responsible for personal, legal, and ethical responsibility for maintaining the security, confidentiality, integrity, and availability at all times of the relevant IT systems. This includes the applications and data held within them.

5.2. Specifically, in terms of IT access, users must ensure that they do not personally attempt to gain unauthorised, malicious and / or illegal electronic access to any of the CCG's IT systems, resources, or materials.

5.3. Specifically, users have a duty of care towards ensuring:

- the prevention of unauthorised, malicious and / or illegal access by any individual to any of the CCG's IT systems, resources and / or materials;
- the prevention of any individual from using any of the CCG's IT systems, resources and / or materials in order to commit or facilitate an offence as defined within the law and / or as advocated within the CCG's documented policies and procedures
- the prevention of unauthorised, malicious and / or illegal modification to, or corruption of, any of the CCG's IT systems, resources and / or materials;
- Unauthorised disclosure of personal confidential information.

5.4. Users must report to their Line Manager any suspicions relating to computer misuse that include:

- any individual attempting to gain access or exceed the access and / or privilege levels to any of the CCG's IT application systems, resources, or materials for which they do not have direct authorisation;
- any individual attempting to use another user's member's ID and password to gain access to any of the CCG's IT application systems, resources, or materials.

5.5. Users must ensure that they do not personally undertake - and prevent wherever possible by reporting suspicions regarding – illegal electronic activities which attempt to utilise, modify or adapt any of the CCG IT systems, resources and / or materials in order to perform activities or functions that represent a breach of national NHS policy and / or UK law, and that are therefore in direct contravention of organisation policies and protocols, including but not limited to:

- proactively sharing account and password details
- attempting to use the CCG Internet and / or email system to receive and / or transmit pornographic, violent, or sexual images;
- attempting to use the CCG network and / or resources to duplicate copyright protected software for personal and / or financial gain;
- attempting to use the CCG network and / or resources to develop, create or perpetuate any form of computer virus or malicious software, including the purposeful uploading or transmission of a known computer virus or item of malicious software to others, whether internal or external to the organisation.

5.6. Users must ensure that they do not personally undertake - and prevent wherever possible by reporting suspicions regarding - potential corruption of the CCG IT assets by any attempt to subvert, amend, modify or otherwise inappropriately compromise or affect, any of the CCG's IT application systems resources and / or materials, including:

- attempting to alter, erase, modify or otherwise compromise, any legitimate software, files, databases or any other form of stored information that is either owned by, been developed by or on behalf of, the CCG's or is under the guardianship of the CCG's without proper and appropriate authority and / or legitimate intent;
- attempting to copy or move any legitimate software and / or associated material to any storage medium other than that which it is intended by the CCG;
- knowingly causing or facilitating damage to any of the CCG IT systems, resources and / or materials, including any attempt to cause or facilitate negative effect to the reliability of any of the CCG's IT application systems,

resources and / or materials;

- preventing, or otherwise hindering, legitimate electronic access by authorised members to either the CCG's IT network and application systems, or to any information held within CCG's IT network and application systems;
- corrupting, or knowingly attempting to corrupt, the accuracy and completeness of any information held within CCG's IT network and application systems.

5.7. Should any users fail to comply with any of these regulations they will be considered to be in breach of the Information Security Policy, and the Computer Misuse Act 1990. This may result in serious disciplinary action being brought against them in line with CCG's disciplinary policy and may lead to the termination of their employment.

6. User Account Control

6.1. All users will be given a unique Login to access the CCG network and systems.

6.2. Before users can gain access to the CCG's IT network (and subsequently any of the CCG's computer applications – including email and internet) authorisation MUST be obtained from a Line Manager. Line Managers must complete and submit a New Starter Requirements Form (Appendix A) available from the corporate office.

6.3. When requesting access for a new starter the line manager must ensure that the new user is provided with the minimum access that is required for them to perform their function.

6.4. For new users domain accounts; NHS Mail accounts and folder access requests can only be made via the IT Helpdesk by the CCG IT Manager, CCG Operations Manager or other named individuals with delegated responsibility (referred to as 'Data Controllers') following approval by the new user's line manager. For access to some folders and information systems the approval by the relevant Information Asset owner will also be required. A minimum of one week's notice is required for the setup of new user accounts. A list of Information Asset Owners and Data Controllers is available from the CCG's IG Lead. Queries around information assets should be directed to the CCG Information Governance Lead or Information Governance support.

6.5. For access to Spine systems users MUST complete the appropriate Registration Authority (RA) forms following advice from the CCG Registration Authority Agent . The application MUST be approved and counter-signed by the Line Manager.

6.6. All relevant changes to an employee's status which require a change to their IT set up or information systems access [e.g. changing a user's folder access or closing a domain account] must be approved by the line manager and where required the Information Asset Owner. The required change should then be communicated to the CCG Data Controllers who will request the change from the CCG's IT provider. Examples of relevant changes are role changes, resignation or termination and other interruptions to continuous employment.

6.7. To prevent users from inappropriate access to information as they move around the organisation it is important that access rights, especially to sensitive information, are reviewed/revoked when moving to a new area/role with any required changes processed as above. Information access should be the minimum required for the user to perform their function. Access to information must not be retained 'just in case' the user's member transitions back into an area.

6.8. On departure from the organisation all users (including secondees, contractors, temporary users and permanent users) will surrender all IT equipment to their line manager including but not limited to, computers, iPads, mobile phones, remote VPN access tokens, encrypted USB sticks.

6.9. It is the responsibility of the line manager to ensure that leavers who depart in a planned manner hand over all CCG information to which they have access. In addition, the line manager should ensure that the user has cleared their H:(Home) Drive and Outlook folders of all information ensuring that relevant corporate information is placed in the appropriate shared folders. Access to specific data once a user has departed in a planned manner will only be made available with express authorisation of the joint Chief Information Officer.

6.10. In circumstances where an individual is unavailable for unforeseen reasons, access to their information/documentation held on CCG equipment may be granted only with the express authorisation of the joint Chief Information Officer. This includes information on:

- laptop
- e-Mail
- network drives
- paper information

6.11. When a user leaves the organisation the domain account should be closed down immediately and the user marked as a 'leaver' on NHS mail. The line manager should inform a CCG Data Controller who will request this action from the CCG's IT provider.

6.12. Users are not permitted to share their, or others, usernames and passwords to gain access to the CCG network or other information systems.

6.13. Users may at their own discretion permit other users (i.e. PA's) to access their e-mail. It is the e-mail owners' responsibility to ensure that such access is appropriate and does not result in individuals having inappropriate access to sensitive information. Further information in regard to this can be found in Email Policy under delegated authority. Please refer to the Email Policy for guidance.

7. Systems Security/Network Usage

7.1. During initial setup of user accounts a temporary password may be created. The communication procedures for these temporary passwords shall ensure the security of passwords at all times. Once issued with a temporary password a user MUST change this at first logging into the system.

7.2. All users must always operate CCG equipment using their username and password. Passwords must meet complexity requirements and MUST NOT be shared with anyone. Logging onto CCG equipment with credentials that users are not authorised to use is not permitted.

7.3. All users shall authenticate themselves using a password at the Windows Login. These passwords will as a minimum comply with the following:

- Changed every 90 Days
- 8 characters long
- Have at least three of the following: number (0-9), special character (e.g.!"£$%) upper case and lower-case character.

7.4. For further guidance on password security refer to Appendix B.

7.5. CCG staff are responsible for the security of their passwords and accounts and are therefore responsible for all computer transactions that are made with their username and password.

7.6. If a password becomes known to another person, it must be changed immediately.

7.7. All access to the CCG network must be provided by the CCG IT service provider at the request of a CCG Data Controller (as set out in clauses 5.1 to 5.4)

7.8. It is mandatory for all users to lock their terminals, workstations, laptops, by pressing ctrl/alt/del (or "windows key" and L), iPads and/or Smartphones when not using their device, even for a short period. As the CCG is implementing agile working, in line with the agreed policy statement that "work is something you do not where you go", it is essential that users lock their screen (as agile working is likely to be at home and or other potential public locations).

7.9. CCG equipment is configured in order to restrict certain user activities. These restrictions are for support, security, and management purposes. Circumvention of these restrictions without appropriate authorisation may lead to disciplinary action.

7.10. Desktop/Laptop software installations must be performed by the CCG IT Provider only. Users are prohibited from installing any software themselves.

7.11. All users must not access or attempt to access information to which they do not have a legitimate business need and to which they have not been authorised to view.

7.12. It is strictly forbidden for users to knowingly browse, search for or look at any information relating to themselves, their own family, friends, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

7.13. All data and information residing on the CCG equipment, (e.g. laptops, mobile phones, etc.) that has been allocated to CCG staff remains the property of CCG at all times.

7.14. The illegal copying of copyrighted content onto CCG equipment is not permitted.

8. Data Storage

8.1. Data must be saved on a network drive. The only circumstance where data may be saved to the hard disk or authorised encrypted removal media is when a laptop is being taken to a site where the CCG network is not accessible. In this event, a copy of all the data must be left on the network as a backup.

8.2. All CCG corporate data should be stored in one of the following locations, and not locally on laptop / desktop hardware:

- CCG Shared Data Drive e.g. 'N' drive
- CCG Personal 'H' Home Drive
- Microsoft SharePoint sites
- Microsoft Teams channels

8.3. Users are not permitted to store personal music or photographs on the CCG's network drives.

9. Guest Wi-Fi Access

9.1. The provision of a 'Guest Wi-Fi' facility at the CCG allows guests and visitors the ability to connect directly to Internet services without compromising the integrity of the CCG network.

9.2. The guest network will be security scanned on a regular basis to ensure that the service is not abused.

10. Internet Usage

10.1. Access to the Internet is provided to support the business, but it may be used for occasional and reasonable personal use e.g. during lunch breaks provided that it does not interfere with the performance of duties and does not conflict with CCG policies.

10.2. Files from the internet, or any images that are displayed must not be downloaded for personal use as there may be any number of issues concerning copyright, viruses, and overall functioning of the computer.

10.3. Instant messages and other communications mechanisms made across the internet may not be secure. CCG authorised communication mechanisms only should be used.

10.4. Transactions are not permitted on sites requiring software to be downloaded before proceeding.

10.5. The CCG accepts no responsibility for any charges or loss incurred in relation to personal purchases or financial transactions using CCG IT facilities regardless of cause.

10.6. To intentionally access or forward material that is defamatory, pornographic, sexist, racist, online gambling or material whose publication is illegal or risks causing offence or disrepute to CCG may lead to disciplinary action or prosecution. If access to restricted material is required, a request to the CCG IT provider with supporting business justification and Line Manager endorsement should be submitted prior to attempting to access the material / site.

10.7. Users must be aware that each website they visit is logged and these logs can be examined to support a disciplinary action.

10.8. The CCG prohibits access to websites deemed inappropriate and monitors access and usage. The monitoring information may be used to support disciplinary action.

10.9. 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.

10.10. If you have any questions about what is considered to be appropriate or inappropriate use, please check with your manager or the IT Department. Known sites falling within the above categories may be blocked by web security software.

10.11. 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.

10.12. The use of the CCG IT systems to conduct on-line selling is strictly prohibited.

10.13. The internet must not be used for participation in online games.

10.14. Messages must not be posted on any internet message board, social networking sites or other similar web-based services that could bring the CCG into disrepute, or which a reasonable person would consider to be offensive or abusive.

11. E-Mail Usage

11.1. The CCG provides email to assist employees, third parties, contractors, and temporary staff in the performance of their jobs and its use should be limited to official CCG business.

11.2. No employees, third parties, contractors and temporary staff should knowingly use the CCG's email system in any way that may be interpreted as insulting, disruptive or offensive by any other person, or which may be harmful to the CCG. This includes forwarding any received email containing any prohibited material listed below.

11.3. Examples of prohibited materials include, but are not limited to:

- sexually explicit messages, images, cartoons, or jokes
- unwelcome propositions, requests for dates, or love letters
- profanity, obscenity, or libel
- ethnic, religious, or racial slurs
- or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.

11.4. Emails concerning illegal activities must not be sent or forwarded unless they relate to the legitimate business of CCG. The CCG Information Governance Lead (IGL) must be notified immediately should any such e-mails be received. These emails must not be forwarded to anyone unless required by IGL.

11.5. The system may not be used for personal financial gain.

11.6. The forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Also, virus warnings come under the same exclusion; the majority of these are false, to check the truth of these messages consult with IGL/ITSG, but do not under any circumstances forward these messages to anyone inside or outside of the CCG.

11.7. All email messages that are sent externally from the CCG will be passed over networks owned by other people; this is not a secure form of communication. If the content of the message could cause embarrassment or problems for the CCG or cause financial loss, should the contents become known, a more secure method should be used.

11.8. The user logged in at a computer will be considered to be the author of any messages sent from that computer. Remember to log-out or lock computers if left unattended (press the “windows” key and the letter “L” key at the same time). Under no circumstances should an e-mail be sent from a PC that is logged in to the network by another person. Email addresses should not be disclosed unnecessarily.

11.9. Disclosing email addresses when filling in surveys or other questionnaires will increase the risk of receiving unwanted junk messages.

11.10. Email should not be used to send large attached files (i.e. 10 Megabytes or larger), unless very urgent. Many email systems including those used by the NHS will not accept large files, which are returned and may result in overloading CCG’s email system. Secure file transfer such as SFTP or removable media, appropriately encrypted, should be used to send large amounts of data, whenever possible.

11.11. Attachments to email messages should not be opened unless they are expected and from a known sender. Extreme caution should be exercised.

11.12. CCG emails must not be automatically forwarded to other non-NHS or Government e-mail addresses e.g. Hotmail, Gmail etc. The CCG provides a number of solutions for accessing the CCG's email system when away from the office. See email policy v1.4

11.13. CCG users must comply with the terms and conditions of the NHSmail service which are available to view at: http://www.connectingforhealth.nhs.uk/systemsandservices/nhsmail/about/aup/index_html/?searchterm=aup

11.14. Users must be aware that CCG may interrogate email accounts and content (including deleted items) without notice if there appears to be a just cause to do so and information can be used to support disciplinary action.

11.15. Person identifiable information, confidential or sensitive information should not be sent via email unless it is encrypted. NHS.net email is automatically encrypted in transit, therefore any email sent from an NHSmail account to another (e.g. xxx@nhs.net to yyy@nhs.net) is secure. The user sending the email must first confirm the recipients email address, for example verbally over the telephone or through the NHS.net directory.

11.16. NHS.net email is hosted on the N3 network and as such forms part of the wider public sector Government Digital Service. This means that email is encrypted when delivered to any of the following email domains:

- gov.uk
- gov.scot
- gov.wales

Note that all gsi-family domain names (gsi.gov.uk, gse.gov.uk, gcsx.gov.uk or gsx.gov.uk) have now been retired since March 2019 as advised by the cabinet office.

11.17. When sending outside the government domain network, person identifiable, confidential, or sensitive information must be removed from the email and sent as an encrypted attachment.

12. Mobile Device Usage

12.1. All mobile devices (laptops, tablets, mobile phones) issued by CCG are intended as a business tool to enable the member of users to perform their role.

12.2. All Users issued with a CCG laptop are required to sign the Laptop User Agreement Form (Appendix C)

12.3. Users are prohibited from installing any additional software on CCG mobile equipment (with the exception of Smartphones – see 12.5 below). All software installation for laptops and tablets must only be carried out by the CCG IT provider.

12.4. Incidental personal usage of corporately issued mobile devices (Voice, SMS, and Data) is permitted under exceptional circumstances. All costs associated with mobile 'apps' will be considered as personal use. The CCG is able to log all usage of mobile devices and should personal usage appear to be excessive this may be investigated further.

12.5. Mobile internet and email access via CCG Mobile devices are subject to the same restrictions as those outlined in sections 9 and 10 above.

12.6. Applications may be installed onto smart phones however support will not be offered for these applications and should these be suspected of causing issues with core business functionality these applications must be removed.

12.7. Users must ensure that all mobile devices are stored securely at all times. In line with the Agile Working Policy (and individuals working across different locations such as working from home), individuals must log off at the end of the working day and ensure that they close down the different systems and applications. Laptops / mobile devices should where possible be kept away from a position where it's contents can be viewed by people not authorised to do so. In addition and in line with agile working policy there may be a requirement to add devices to home insurance mandates.

12.8. Users of mobile computing devices must not allow unauthorised access by third parties including, but not limited to, family and friends.

12.9. Passwords relating to mobile devices should never be written down and/or kept with the device.

12.10. Mobile devices must be transported securely and may only be left in the boot of a car during the day when there is no alternative method of securing the device. Devices must not be left in any vehicle overnight.

12.11. The antivirus software must be kept up to date by regular connection (at least every 30 days) to the secure CCG Network.

12.12. All Mobile computing devices (tablets and laptops) are encrypted. In order to ensure synchronisation all devices must be connected to the secure CCG network at least every

30 days.

12.13. No peripheral device of any kind (e.g. digital cameras, PDAs, USB pen drives, etc.) may be installed or configured on any CCG computer.

12.14. Under no circumstances should person identifiable data be copied to the C: drive on a laptop or tablet device.

12.15. If a mobile device is lost or stolen then it should be reported to the IT helpdesk and Line Manager as soon as possible.

12.16. Employees and users of CCG systems and equipment are not permitted to take their IT equipment / devices and use them outside of the UK unless they have been granted appropriate permission from the Head of IT.

13. Additional Responsibilities for Line Managers

13.1. All Line Managers have a duty to meet the obligations as users but in addition, they have additional responsibilities as line managers of CCG users (including contractors). These include:

- Ensure users maintain adequate protection of their systems and equipment at all times particularly when left unattended.
- Ensure all staff have a copy of this policy.
- Ensure that all temporary, agency and contracted staff have time-limited access to systems based on their role
- Users' access is revoked and equipment returned when users move departments / leave the organisation.

14. Remote Access

14.1. The CCG IT provider supports agile working by providing a remote access service to enable users to connect remotely to the CCG network when they are not at a CCG office location.

14.2. Remote Access functionality is not provided to all users by default. Should this service be required it should be requested by the user's Line Manager.

14.3. When working from home users should ensure that they have the appropriate facilities to support Remote Access to the CCG network i.e. their own broadband connection.

15. Distribution and Implementation

15.1. This document will be made available to all users via a CCG e-mail Communication to notify them of the release of this document and any subsequent updates.

15.2. This document must be made available to all new starters prior to being given access to CCG IT equipment, network, and systems.

15.3. All users will be required to sign the declaration in Appendix C

16. Microsoft Teams

16.1. To allow individuals to work in a more accessible way, Microsoft Teams has been permitted as an appropriate application for staff across the NHS to use. The Microsoft Teams application has been installed on user's laptops and this acts as a way for meetings to held virtually as well as messages and files shared across different directorates and NHS staff. Although Microsoft Teams has been approved as an appropriate system to use, staff should continue to follow the necessary supporting policies and procedures (Information Security, Acceptable Use of IT, Confidentiality and Code of Conduct etc) to ensure no breaches and that the policies are followed appropriately.

17. Monitoring

17.1. Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Lead, together with independent reviews by both Internal and External Audit on a periodic basis.

17.2. The CCG IG Lead is responsible for the monitoring, revision and updating of this document.

17.3. This policy will be reviewed at least annually, and in accordance with the following as required:

- legislative changes
- good practice guidance
- case law
- significant incidents reported
- new vulnerabilities
- organisational changes

18. Equality Impact Assessment

18.1. As part of its development this document and its impact on equality has been analysed and no detriment identified.

Appendix A – Bury CCG New Starter Requirements

NHS
Bury
Clinical Commissioning Group

BURY CCG INTERNAL NEW STARTER REQUIREMENTS FORM

To be completed by the Line Manager at least 2 weeks before the start date, this form applies to CCG employees and agency staff. Please return the completed form to the Corporate Office via email to buccg.corporateoffice@nhs.net

1	**NEW STARTER NAME**	
	Title	
	First Name	
	Last Name	

2	**ROLE**	
	Job Title	
	Team (Corporate, Finance etc.)	

3	**EMPLOYMENT**	
	Employer (Bury CCG or Agency name)	
	Start Date	
	Contract Type	Permanent ☐ Temporary ☐ Fixed Term ☐
	Contract End Date (if Temporary or Fixed Term)	

3	**IT REQUIREMENTS**		
	Existing NHS Mail Account (postholder required to arrange for account to be deactivated at previous organisation)	Yes ☐ No ☐	
		If yes please specify email address:	
	Network Log in Account Required (access to the network)	Yes ☐ No ☐	
	Folder Access Requirements (Manager must obtain approval from information asset owner)	Specify all folders required e.g. N:\All Staff etc	
	Hardware Requirements (Finance must authorise any costs)	Laptop ☐ Keyboard ☐ Screen/Monitor ☐ Mouse ☐ Docking Station ☐	
	Transfer of Existing Asset (laptop) - If yes please specify details	Yes ☐ No ☐	
		Asset Number:	
		Name of previous user:	
	Additional Software requirements (Finance must authorise any costs)	Specify exact software required if this differs from standard:	
	Mobile Phone required	Yes ☐ No ☐	

4	**RESOURCES**	
	ID Cards Required	Yes ☐ * No ☐ *please complete request for Identification Badge at the end
	Smart card required	Yes ☐ * No ☐ *please approach your team's smartcard sponsor

5	**AUTHORISATION**	
	LINE MANAGER	
	Name	
	Job Title	
	Signature	
	Date	
	INFORMATION ASSET OWNER (MUST BE AUTHORISED FOR ACCESS TO N: DRIVE FOLDERS)	
	Name	
	Job Title	
	Signature	
	Date	

6	**FURTHER AUTHORISATION** **(REQUIRED IF A COST IS IDENTIFIED FOR EQUIPMENT/ ADDITIONAL SOFTWARE)**	
	BUDGET HOLDER	
	Name	
	Job Title	
	Signature	
	Date	
	FINANCE	
	Name	Faisal Ghazi
	Job Title	Management Accounts
	Signature	
	Date	

PLEASE ENSURE ALL REQUIRED SIGNATURES ARE OBTAINED PRIOR TO SUBMITTING THIS FORM FOR PROCESSING TO AVOID DELAY.

NHS
Bury
Clinical Commissioning Group

REQUEST FOR IDENTIFICATION BADGE

Please use this form to request a staff ID badge. Upon completion please return to the Corporate Team via email buccg.corporateoffice@nhs.net for processing.

ID should be worn at all times whilst on NHS Bury CCG business. The card will remain the property of NHS Bury CCG and will be programmed for entrance to sites as listed below. In the event of loss please contact the Corporate Office as soon as possible, the card will then be deactivated and a replacement can be requested although a charge may be made. On termination of employment all cards should be returned to the line manager via the exit interview and then returned to the Corporate Team.

Name	
Job Title	
Base	
Contact Telephone Number	
Start Date	
Contract Type **(tick relevant box)**	Permanent □ Temporary □ Fixed Term □
Contract end date **(if Temporary or Fixed Term)**	
Access required to **(please indicate)**	Townside □ 3KP/Town Hall □
Replacement reason **(if replacement card)**	
Managers Name	
Managers Signature	
Date	

For office use only:	
Form received by (name)	
Date received	
ID card spreadsheet updated	Yes □ No □
Card received by user	
Signature	
Print Name	
Date received	

Appendix B – Password Good Practice Guidance

- Poor and weak passwords have the following characteristics:
    - The password contains less than eight characters
    - The password is a word found in a dITionary (English or foreign)
    - The password is a common usage word such as:
        - Names of family, pets, friends, co-workers, fantasy characters, etc.
        - Computer terms and names, commands, sites, companies, hardware, software.
        - Birthdays and other personal information such as addresses and phone numbers.
        - Word or number patterns like “aaabbb”, qwerty, zyxwvuts, 123321, etc.
        - Any of the above spelled backwards.
        - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

- Strong passwords have the following characteristics:
    - Contain both upper- and lower-case characters (e.g., a-z, A-Z)
    - Have digits and punctuation characters as well as letters e.g., 0-9,
    - Are at least eight alphanumeric characters long.
    - Are not words in any language, slang, dialect, jargon, etc.
    - Are not based on personal information, names of family, etc.

- Passwords must never be written down or stored online.

- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: **"TmB1w2R!" or "Tmb1W>r~" or some other variation.**

- Do not share CCG passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential CCG information.

- Here is a list of password ‘don'ts’:
    - Don't reveal a password to anyone.
    - Don't reveal a password in an email message.
    - Don't talk about a password in front of others.
    - Don't hint at the format of a password (e.g., "my family name").
    - Don't reveal a password on questionnaires or security forms.
    - Don't share a password with family members.
    - Don't reveal a password to co-workers while on leave.
    - Don’t use the "Remember password" feature of applications (e.g., Internet explorer).

- If an account or password is suspected to have been compromised, report the incident to the CCG IG Lead and change all passwords.

- Any queries regarding passwords or changing of passwords must be referred to the CCG IG Lead.

NHS
Bury
Clinical Commissioning Group

Laptop User Agreement Form

Name:		Job Title:	
User ID:		Department:	
Asset No			

In accepting the use of the Bury CCG laptop detailed above and as the 'authorised asset user', I agree to the following conditions:

- I understand that I am solely responsible for the laptop device at ALL times whether this is on NHS premises, the premises of other organisations, on public transport or at home.
- When not in use it will be my responsibility to ensure that the laptop is kept in a lockable drawer/cupboard or a secure office
- Whilst in transit the laptop will be in a suitable carrying case and kept out of view wherever possible. I will not leave the laptop unattended in a public place or in a vehicle overnight.
- I will not keep password details and/or my remote access VPN token in the same location as the laptop
- I will use the laptop only in connection with Bury CCG business
- I will not install/download any unauthorised software and /or applications
- I will not allow the laptop to be used by an unknown or unauthorised person. I assume the responsibility for the actions of others while using the laptop
- I will abide by the CCG Acceptable Use of IT and associated policies.

As an authorised asset user you should be aware of the following conditions:

- If the laptop is lost stolen or damaged, the incident must be reported to the CCG IT Provider Service Desk. If stolen the police crime reference number must also be provided.
- The antivirus software must be kept up to date by regular connection (at least every 30 days) to the secure CCG Network.
- No personal confidential data/sensitive data must be stored on the local hard drive. Any information that needs to be saved should be stored on the organisation's network.
- No external devices will be connected to the laptop, unless proved by the CCG IT provider. Only approved 'Safesticks' are permitted - DO NOT use your own as they may not be secure and you could unknowingly be bringing virus' into the CCG.
- When the laptop is no longer required or when the asset user leaves the CCG employment it must be returned to the CCG.

I agree to use the laptop allocated to me in accordance with the CCG Acceptable Use of IT Policy and the above conditions.

Print Name:			
Signature:		Date:	

Appendix D – User Declaration

NHS
Bury
Clinical Commissioning Group

Bury CCG Acceptable Use of IT Policy – User Declaration

Name:		Job Title:	
User ID:		Department:	

- I agree to use the IT equipment made available to me by Bury CCG in accordance with the CCG Acceptable Use of IT Policy.

- I have seen, read and understood NHS Bury CCGs Acceptable Use of IT Policy.

- I understand the terms of the policy and agree to abide by them.

- I understand that audit and security software may monitor and record the use I make of IT systems, Internet and email, which may include logging the address of web sites that I access.

- I understand that Non-compliance with the clauses in this policy may result in disciplinary action.

Print Name:			
Signature:		Date:	