NHS
Nottingham and
Nottinghamshire
Integrated Care Board

Account Management and Access Policy

July 2022 – July 2025

CONTROL RECORD			
Reference Number GOV-012	**Version** 1.0	**Status** Final	**Author** Cyber Security Assurance Programme Board
			Sponsor Information Governance Steering Group
			Team Information Governance Team
Title	Account Management and Access Policy		
Amendments	None		
Purpose	To prevent and control unauthorised access to the Integrated Care Board's information systems and the shared network.		
Superseded Documents	None		
Audience	All staff, third parties, contractors and partners, that are users of systems, devices or applications supplied to them by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions.		
Consulted with	The Policy has been reviewed and developed by the Cyber Security Assurance (CSA) Delivery Group and approved by the CSA Programme Board.		
Equality Impact Assessment	June 2022		
Approving Body	ICB Board	Date Approved:	1 July 2022
Date of Issue	July 2022		
Review Date	July 2025		
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.			

NHS Nottingham and Nottinghamshire Integrated Care Board (ICB)'s 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 nnicb-nn.comms@nhs.net.

Contents

1. Introduction

1.1. This policy applies to the account management and access to systems, devices, applications and services deployed in support of NHS or health and social care business functions and provided by Nottinghamshire Health Informatics Service (NHIS) on behalf of Nottingham and Nottinghamshire Integrated Care Board (ICB).

1.2. Where hardware and software (operating systems, programmes/applications and devices) are not securely configured the number of potential vulnerabilities is increased. This can make systems that support business functions more at risk of not only being attacked but exploited resulting in data breaches, loss of service and reputational damage. NHS organisations are required to have, or contractually require from suppliers, that its IT systems are configured as securely as possible.

1.3. Nottingham and Nottinghamshire ICB Directors, Heads of Departments, Senior Managers nominated Information Asset Owners and Information Asset Managers are responsible for the security of their systems, devices or applications supplied to their business area by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions. This includes determining the level of access to be granted to specific individuals to their business environments where information is processed or stored.

1.4. Furthermore, they are responsible for ensuring that all staff permanent, temporary and contractor:

- are aware of the information governance and information security policies, procedures and user obligations applicable to their area of work
- are aware of their personal responsibilities for information security.
- have appropriate training for the systems they are using
- know how to access advice on information security matters

1.5. Inactive user accounts may appear docile, but can cause significant impact on the ICB operationally, especially where they are not disabled or remain on the system without expiry limits. Outside intruders trying to hack into an organisation can use these accounts and the activities potentially remain undetected. Employees who leave the organisation or transfer departmentally can misuse their login credentials to access network resources.

1.6. The damage that can be done to the network depends on the skill of the intruder and the number and level of privileges they have. If a user can still log into servers, access confidential data, or even just access the organisations resources, they can wreak havoc that can cause reputational damage and breach data protection legislation.

2. Purpose

2.1. This purpose of this policy is to prevent and control unauthorised access to the ICB's information systems, devices, applications and services and the shared network. The policy describes the registration and de-registration process for all information systems and services provided by Nottinghamshire Health Informatics Service (NHIS) on behalf of Nottingham and Nottinghamshire ICB and management of system access accounts.

2.2. Effective access to systems controls work on the principle of 'least privilege'. Least privilege means giving a user the lowest level of privileges which are essential to perform its intended function; this applies to everyday users and to system and application administrators. Its aim of applying least privilege is to enhance the protection of data and information processed and the IT/software functionality from faults and malicious behaviour

2.3. This policy describes how access controls are applied by the organisation, covering all stages in the life cycle of user access, from the initial registration process to the final de-registration of users who no longer require access to the organisations information systems and services.

2.4. This policy covers all devices owned or connected to the IT network at any site owned or leased by the Nottingham and Nottinghamshire ICB or from a remote location from where ICB staff may connect to this network.

2.5. Permission may also be granted for users to remotely access information systems from non-NHS sites/private homes using Remote Desktop Access (Virtual Private Network) and the same security principles will apply.

3. Scope

3.1. The Account Management and Access Policy applies to:

- All employees who work for or on behalf of the Nottingham and Nottinghamshire ICB including those on temporary or honorary contracts, secondments, volunteers, Integrated Care Board members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the ICB.

- All Nottingham and Nottinghamshire ICB Directors, Heads of Departments, Senior Managers nominated Information Asset Owners and Information Asset Managers are responsible for the security of their systems, devices or applications supplied to their business area by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions.

4. Definitions

4.1. Account Management and Access Policy definition:

Term	Definition
Account Management and Access Policy	Sets out the organisational process providing individuals with access to systems, applications and resources in all stages of access life-cycle such as requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorisations; and managing these functions. **Access controls include:** • disable/remove or limit system utilities that are capable of overriding application or system controls • control system access rights of other applications • manage the use of privileged access • remote access to systems **Account Management** • authorising access based on current role and responsibilities and using system level basis • granting initial access • periodically reviewing access granted • changing access as user roles change (e.g., job responsibilities change) • removing access from users who no longer require access (e.g., termination, transfer to another business area) • establishing, resetting, and expiring authentication. **Account management includes:** • documentation of account and authentication management procedures • segregation of duties from authorisation to managing accounts • communication to user about use and responsibilities for maintaining the account and authentication • periodic review of accounts

5. Roles and Responsibilities

5.1. This section should state the key responsibilities for specific roles and staff groups in relation to delivering the documents objectives. If table is to be used, use the below format:

Role	Responsibilities
ICB Board	The Board must have Individual Officer arrangements in place to ensure that requirements of this policy are carried out effectively.
Senior Information Risk Owner (SIRO)	The Chief Financial Officer, in their role as Senior Information Risk Owner (SIRO) takes ownership of the organisation's information risk and act as an advocate for information risk on the Board.
Information Governance Steering Group (IGSG)	IGSG reports to the Audit and Risk Committee and is responsible for ensuring that this policy is implemented, including: • Providing management direction and support for Account Management and Access activities in accordance with business requirements • Ensuring additional guidance and training deemed necessary to support Account Management and Access activities are implemented • It will monitor and provide Board assurance in this respect.
Information Asset Owner's (IAOs) / Directors	Are responsible for implementing and maintaining this policy in their area of management of Nottingham & Nottinghamshire ICB systems, devices or applications, ensuring that procedures are in place and staff have adequate access to information management and security training.
Designate Heads of Department and Senior Managers	Are responsible for implementing and maintaining this policy in their area of management of Nottingham & Nottinghamshire ICB systems, devices or applications ensuring that procedures are in place and staff have adequate access to information management and security training.
Information Asset Managers (IAMs) and line managers	Information Asset Managers (IAMs) have day to day responsibility for managing their information assets and associated records management, confidentiality, integrity and availability to include information security.

Role	Responsibilities
All Staff	All members of staff should read and note and fully adhere to the requirements of this policy and must have access to and follow the guidance outlined in related local SOPs/Processes and procedures. The ICB will investigate all suspected/actual security breaches and report through their incident reporting procedures.
Caldicott Guardian	The Caldicott Guardian will be central to the framework for handling personal confidential data in the NHS and will be fully aware of their responsibilities specified in the Caldicott Guardian Manual (Department of Health, 2017 Manual).

6. Account Management and Access Management and Controls

6.1. Principles

- The line manager of the relevant employee is responsible for performing the tasks associated with initial registration, user change and final removal of the user. The NHIS Service Desk will action requests to process account amendments upon the appropriate instruction from the ICB.
- It is the responsibility of the system administrator/information asset manager to ensure that housekeeping tasks are undertaken on the system on a regular basis (such as review of current users and access rights).
- All individuals who access, use or manage the systems provided by the ICB and NHIS are responsible for reporting any breach of this policy to their line-manager, the Information Governance Team and the NHIS Service Desk according to the requirements of the ICB Incident Reporting and Management Policy.
- Identification and authentication shall be used to identify and prove which users have accessed and utilised the organisation's systems and the data within them.
- The degree of authentication (single or 2 factor) shall be assessed for the level of protection required for the processed information and the risk factors to it by the Information Asset Owner (IAO) and Senior Information Risk Owner (SIRO). Where it is deemed 2 factor authentication is required, the authentication mechanisms shall be provided by different methods – e.g., password and token.
- Passwords shall be used to ensure that access to NHS systems, devices and information is controlled and restricted to approved and authorised users only. Passwords shall be complex in nature and follow ICB guidance and best practice.

- Systems should be configured to force the change of passwords at regular intervals. These intervals should be of sufficient frequency to aid security, but not too frequent that this causes problems for users and administrators.

6.2. Granting User Access

- Access to ICB and NHIS managed information systems is controlled through a formal user registration process as detailed in organisational induction and an on boarding process supported by the Information Governance and Security Policies in place at that organisation.
- Each user, including third parties accessing ICB and NHIS hosted systems, is identified by a unique user ID so that users can be linked to and held accountable for their actions.
- Access to managed and supported systems provided by the NHIS Service can be requested via Service Desk through the customer portal and can only be permitted after proper procedures are completed by the employing organisation. The ICB is responsible for requesting an account through the NHIS Customer Portal, or by email to the NHIS.servicedesk@notts-his.nhs.uk
- For system/network accounts, a new user will be set up on receipt of the instruction to the NHIS Service desk. Login details and passwords will only be provided to the owner of the account (or line manager if this is set up prior to commencement in post).
- On first logon to a new user account, the user must change the default password assigned to the account. Logon details must not be shared with others and an individual's account must not be used as a generic account.
- Any access request to a network shared drive area that is not given by default will only be granted following approval from the line manager or a designated staff member. Access requests to restricted folders must be authorised by the folder owner or a designated staff member along with details of the access permissions required.
- Generic or shared accounts will not be set up unless a valid business reason can be given and the organisation has the appropriate governance in place. These accounts must have a valid business user associated with them. Generic accounts (accounts that are not attributed to a single user) do not facilitate an audit trail, in that there is no way to determine who was using the account at any particular time unless a separate log is kept. It is also difficult to attribute particular actions to an individual (for example, accessing an inappropriate website).
- Requests to systems that are not supported by NHIS must be requested from the relevant IAO of that system and account management procedures

documented in the relevant Standard Operating Procedure (SOP) or process or procedure for that business area.

- Remote access may be granted to fulfil an organisation's business needs as described in their information security policies. The requirements for user registration and de-registration remain the same as standard network users.

6.3. Modifying or Moving User Accounts

- Where an employee moves departments within the organisation, the previous line manager is responsible for revoking access to systems that are no longer appropriate for the new role.
- The relevant business area must manage movers within the department.
- Requests to the NHIS Service Desk must provide specific detail of the existing and amended access rights in order for the change to be actioned. Contractors and Temporary staff must have an expiry date allocated at which point the account will be disabled.
- Employers of temporary staff, contractors and placements will request an account through the NHIS Service Desk. These accounts must can be set with an expiry date, at which point the account will be disabled, unless NHIS is informed otherwise.
- Where there is a possibility that a user will return after a long period of absence, the line manager can request re-enablement of the account.
- A list of movers to be circulated to the system administrators/information asset managers so that access can be revoked.

6.4. Removal (leavers) of User Access – Account Termination

- It is the responsibility of a leaver's line manager (or other agreed local organisational process) to notify the NHIS Service Desk that a member of staff has left the organisation and the account is to be disabled.
- The organisation's Service Line Manager will institute a review of all system access rights for employees at the exit interview or upon receipt of resignation notification. All physical equipment must be retrieved including laptops, phones, ID Cards, security tokens and other equipment provided by the organisation.
- The request should be made in advance of the users last day and date to be disabled will follow the system's service level agreement deadline.
- Access to third party services and assets (VPN) will all be disabled. The systems where shared passwords are implemented should be reviewed and passwords changed by the line manager (or IAO/IAM upon notification).

- The email account will be disabled by the NHS mail Local Administrator (NHIS) and an Out of Office set up or divert, whichever is the most applicable.
- For immediate termination or dismissal, the Service Desk must be informed by an authorised Senior Manager/Director by telephone to initiate immediate disablement of accounts.
- List of leavers to be to be circulated to the system administrators/information asset managers so that access can be disabled.

6.5. Privileged User Account Management

- Privileged User Accounts are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include administrative and super user accounts.
- The unnecessary allocation and use of special privileges are often found to be a major contributing factor to the vulnerability of systems that have been breached.
- Access to systems must be relevant and commensurate with the business need of the organisation. That is, the minimum access that satisfies the business need must be given. Privileged access is used by individuals undertaking designated tasks within the job role and are only used for the purposes of system administration.
- Privileged accounts must be authorised by the IAO/IAM for the system, and where applicable requested through the NHIS Service Desk for systems provided by NHIS. Access rights must be reviewed periodically by the IAO/IAM at an agreed frequency to ensure that they remain fit for purpose and access is withdrawn where the circumstances no longer warrant access.
- SOPs, processes or procedures must be developed for the system administrators for each of the applicable systems, setting out how housekeeping and regular review and proactive monitoring of accounts and when this will occur.

6.6. Review of User Account Access Rights

- Line managers or designated staff members must ensure that access to clinical and IT systems is reviewed and revoked for staff members transferring from their department or services.
- A housekeeping report will be run on an agreed basis to ensure that user accounts are not being retained inappropriately. This will be undertaken by the

information system manager / information asset administrator or by NHIS under instruction by the Information Asset Owner (IAO).

- Any user account that cannot be positively identified as current must be disabled pending confirmation of deletion from the organisation employer. To allow for maternity leave and other periods of extended absence, status of users will be ascertained before permanent deletion of accounts.
- The only exception to this will be where a line manager informs NHIS that the account should be retained, gives a reason why and has appropriate authorisation from the Information Governance Team or the Senior Information Risk Owner (SIRO).

6.7. Deletion of Accounts

- Accounts will initially be disabled on notification of a leaver or receipt of a leavers list from the organisation within an agreed period of the leaving date (this will be set out in the SOP, process or procedure for the system). The accounts will be removed from all group memberships and generic accounts.
- Information and Clinical Systems user account deletion requests that come through from an individual (line-manager) are assigned a Sev3 (up to 4wks), the HR leavers list is assigned a Sev4 (up to 3mths) for these requests to be processed.
- The accounts will be retained for an agreed time and then deleted permanently from the system. After this period, any data maintained by NHIS (including Home/G Drive) will be deleted. Currently most clinical systems do not have a permanent delete option, as this would affect auditing/historic data. Accounts are just made inactive or archived.
- The only exception to this will be where a line manager informs NHIS that the account should be retained, gives a reason why and has appropriate authorisation from the Information Governance Team or the Senior Information Risk Owner (SIRO).

6.8. Monitoring and Auding of Inactive Accounts

- Removal of inactive accounts is essential for the security of information systems. It may be preferable to retain accounts in disabled mode before deleting them permanently. If this is the case and has been authorised by the organisation, the password will be reset.
- Access requests to NHIS by an organisational leaver after the leave date but before the deletion date will only be granted upon appropriate authorisation from the employing organisation, such as line manager or head of department. Access will be granted for 7 days only.

- Access request by a current staff member to an account belonging to an exited staff member will be granted depending on the business need and the appropriate written authorisation from the employing organisation, including the Information Governance Team.
- Specific procedures to be put in place for systems managed by the ICB to monitor and review disablement of inactive accounts.

7. Communication, Monitoring and Review

7.1. Managers are required to make staff aware of their information governance responsibilities with ICB information governance related policies to include this Account Management and Access Policy during their induction period. This policy is included in the ICB suite of policies available on-line

7.2. The Information Governance Steering Group are responsible for monitoring compliance and the effectiveness of this policy though the reporting of incidents, use of audits and staff surveys.

7.3. 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 Information Governance Team.

8. Staff Training

8.1. Nottingham and Nottinghamshire ICB is required to ensure organisational compliance with legislation and Department of Health and Social Care guidelines relating to data security and data protection. This requires knowledge and awareness of data security and data protection to be at the core of the ICBs objectives and embedded amongst other governance initiatives.

8.2. Annual Data Security Awareness (DSA) Level 1 training, as developed by NHS Digital, is mandatory for all staff members, including new starters, locums, temporary staff, lay members, student and contract staff at induction and on an annual basis as refresher training for staff.

8.3. This training is mandated for corporate induction and thereafter annually with a minimum target of 95% completion across the ICB. At Induction managers must provide staff with the Information Governance Staff Handbook that provides awareness of information security concepts & principles to ensure compliance with this policy but should more training be required please contact the Information Governance Team.

9. Equality and Diversity Statement

9.1. Nottingham and Nottinghamshire ICB pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation as a commissioner and provider of services, as well as an employer.

9.2. The ICB is committed to ensuring that the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary), marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.

9.3. We are committed to ensuring that our activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people 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.

9.4. As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

9.5. 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.

10. Interaction with other Policies

10.1. This policy document should be read in conjunction with:

- Confidentiality and Data Protection Policy
- Information Security Policy
- Internet and Email Policy
- Removable Media Policy
- Acceptable Use of the Network Policy
- Risk Management Policy
- Incident Reporting and Management Policy
- Information Governance Staff Handbook

11. References

11.1. This policy takes into account reviews of the following as part of the development of this policy document:

- Access to Health Records Act 1990
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Data Protection Act 2018
- General Data Protection Regulation 2016
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Equality Act 2010
- Fraud Act 2006
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- NHS Digital Guidance
- Human Rights Act 1998
- ISO/IEC 27001:2005 Specification for an Information Security Management system & ISO/IEC27002:2005 Code of Practice for Information Security Management
- NHS Act 2006 and
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- 2004 Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992.

12. Equality Impact Assessment for this Policy

Date of assessment:	**June 2022**			
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.
Age[1]	None identified	N/A	None	None
Disability[2]	None identified	N/A	None	None
Gender identity (trans, non-binary)[3]	None identified	N/A	None	None
Marriage or civil partnership status[4]	None identified	N/A	None	None
Pregnancy or maternity[5]	None identified	N/A	None	None
Race[6]	None identified	N/A	None	None

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

[2] 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.

[3] The process of transitioning from one gender to another.

[4] 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'.

[5] 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.

[6] 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.

Date of assessment:	**June 2022**			
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.
Religion or belief[7]	None identified	N/A	None	None
Gender[8]	None identified	N/A	None	None
Sexual orientation[9]	None identified	N/A	None	None
Carers[10]	None identified	N/A	None	None

[7] 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.

[8] A man or a woman.

[9] 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

[10] Individuals within the ICB which may have carer responsibilities.