**Access Control Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| 1.0 | June 22 |  | AJH |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 3](#_Toc96236545)

[1.1 Guidance statement 3](#_Toc96236546)

[1.2 Status 3](#_Toc96236547)

[1.3 KLOE 3](#_Toc96236548)

[1.4 Training and support 4](#_Toc96236549)

[2 Scope 4](#_Toc96236550)

[2.1 Who it applies to 4](#_Toc96236551)

[2.2 Why and how it applies to them 5](#_Toc96236552)

[3 Definitions 5](#_Toc96236553)

[3.1 Users 5](#_Toc96236554)

[3.2 Privileged users 5](#_Toc96236555)

[4 Policy statement 5](#_Toc96236556)

[4.1 Principle of least privilege 5](#_Toc96236557)

[4.2 Generic identities 6](#_Toc96236558)

[4.3 Access control methods 6](#_Toc96236559)

[4.4 User access account management 6](#_Toc96236560)

[4.5 Password management 7](#_Toc96236561)

[4.6 System configuration 7](#_Toc96236562)

[4.7 Remote access 7](#_Toc96236563)

[4.8 Wireless access 8](#_Toc96236564)

[4.9 Access control for mobile devices 8](#_Toc96236565)

[4.10 Publicly accessible content 8](#_Toc96236566)

[4.11 Monitoring user access 9](#_Toc96236567)

[5 Responsibilities 9](#_Toc96236568)

[5.1 Senior Information Responsible Owner (SIRO) 9](#_Toc96236569)

[5.2 Managers 9](#_Toc96236570)

[5.3 Users 9](#_Toc96236571)

[6 Compliance 9](#_Toc96236572)

[Annex A – Register of all IG roles/Responsible Persons 11](#_Toc96236573)

# Introduction

## Guidance statement

This policy is to provide a framework for how user accounts and privileges are created, managed and deleted.

It includes how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorised privileges or access.

## Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](https://www.gov.uk/guidance/equality-act-2010-guidance). Consideration has been given to the impact this policy might have with regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

## KLOE

The Care Quality Commission would expect any primary care organisation to have a policy to support this process and this should be used as evidence of compliance against CQC Key Lines of Enquiry (KLOE)**.**

Specifically, Grey Road Surgery will need to answer CQC key questions on “Safe”, “Effective” and “Well-Led”.

The following is the CQC definition of Safe:

*By safe, we mean people are protected from abuse\* and avoidable harm. \*Abuse can be physical, sexual, mental or psychological, financial, neglect, institutional or discriminatory abuse*

|  |  |
| --- | --- |
| **CQC KLOE S6** | Are lessons learned and improvements made when things go wrong? |

The following is the CQC definition of Effective:

*By effective, we mean people’s care, treatment and support achieves good outcomes, promotes a good quality of life, and is based on the best available evidence.*

|  |  |
| --- | --- |
| **CQC KLOE E3** | How does the service make sure that staff have the skills, knowledge and experience to deliver effective care, support and treatment? |

The following is the CQC definition of Well-Led

*By well-led, we mean that the leadership, management and governance of the organisation assures the delivery of high-quality and person-centred care, supports learning and innovation and promotes an open and fair culture.*

|  |  |
| --- | --- |
| **CQC KLOE W4** | Are there clear responsibilities, roles and systems of accountability to support good governance and management? |
| **CQC KLOE W5** | Are there clear and effective processes for managing risks, issues and performance? |
| **CQC KLOE W8** | Are there robust systems and processes for learning, continuous improvement and innovation? |

## Training and support

The organisation will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

# Scope

## Who it applies to

This document applies to all employees, partners and directors of the organisation. Other individuals performing functions in relation to the organisation, such as agency workers, locums and contractors, are encouraged to use it.

Furthermore, it also applies to clinicians who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS).[[1]](#footnote-1)

There are some access roles that require the implementation of stronger controls than those for standard users.

## Why and how it applies to them

* Confidentiality – Systems and information will only be accessible to authorised persons.
* Integrity – The accuracy and completeness of systems and information are

safeguarded.

* Availability – Systems and information are physically secure and will be accessible to authorised persons when required.

Confidentiality, integrity and availability are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital that authorised users who have access to both systems and information at this organisation are aware of and understand how their actions may affect security.

# Definitions

* 1. **Users**

This is the collective term used to describe all those who have access to the Grey Road Surgery’s business information and clinical information systems. An Access Control Register should be used to provide the number of persons allocated each organisational role for each system as part of the evidence requirements for the Data Security and Protection Toolkit submission (see [Annex A](#_Appendix_A_–)).

* 1. **Privileged users**

A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard users are not authorised to perform.

This includes a standard user with approved elevated privileges that allows equivalent access to that of a privileged user.

# Policy statement

* 1. **Principle of least privilege**

Access controls must be allocated on the basis of business need and ‘least privilege’. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil

their business role.

* 1. **Generic identities**

Generic or group IDs shall not normally be permitted as means of access to this organisation’s data but may be granted under exceptional circumstances e.g., for training systems. Generic identities will never be used to access confidential data or personally identifiable data.

* 1. **Access control methods**

Access control methods used by default include:

* Explicit logon to devices
* Windows share and file permissions to files and folders
* User account privilege limitations
* Server and workstation access rights
* Firewall permissions
* Network zone and VLAN ACLs
* IIS/Apache intranet/extranet authentication rights
* Organisation user login rights
* Database access rights
* Encryption at rest and in transit
* Any other methods as contractually required by interested parties

Access control applies to all organisation-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of Grey Road Surgery.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within the organisation’s Active Directory domains. A review period will be determined for each information system and access control

standards will be reviewed regularly at those intervals.

* 1. **User access account management**

User account management procedures must be implemented for user registration,

modification and de-registration on all organisation information systems. These procedures must also include processes for monitoring redundant and inactive accounts.

All additions, deletions, suspensions and modifications to user access should be

captured in an audit log (see [Annex B](#_Appendix_B_–)) showing who took the action and when. These procedures shall be implemented only by suitably trained and authorised

employees.

Access to organisational information systems must be controlled by an approved

authentication method supporting a minimum of a user ID and password combination that provides verification of the user’s identity.

Users shall have a user ID for their sole use for access to all computing services. All individual user IDs must be unique for each user and never duplicated. All user accounts that have not been accessed for an agreed period, without prior arrangement, must be automatically disabled.

All administrator and privileged user accounts must be based upon job function and authorised by the line manager and/or practice manager with the appropriate system administrator declaration completed as indicated in the organisation’s [Systems Administrator Policy](https://practiceindex.co.uk/gp/forum/resources/system-administrator-policy.1783/).

All changes to privileged accounts must be logged and regularly reviewed. Procedures shall be established for all information systems to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role or a user leaves the organisation.

* 1. **Password management**

Passwords must not be shared with any other person for any reason. All default system and vendor passwords must be changed immediately following installation.

All information systems must support strong password management techniques (such as length, complexity, aging, history, account lockout). Additionally, all information systems must technically force new user accounts to change the initial password upon first use to a strong password and thereafter on a regular basis.

* 1. **System configuration**

For audit purposes, systems shall be configured to capture the unique user identity being used. Where technically possible, all standard accounts that are delivered with operating systems shall be disabled, deleted or have their default passwords changed on system installation.

Staff and contractors shall only be granted access to those application functions required to conduct their roles and access to information in applications in accordance with business access requirements and policy. Furthermore, they shall only have access to sensitive systems if there is a business need to do so and they have successfully completed any additional necessary vetting processes.

Sensitive systems should be physically or logically isolated in order to meet the requirements of restricted access to authorised personnel.

* 1. **Remote access**

The organisation shall:

* Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed
* Authorise remote access to the information system prior to allowing such connections
* Ensure that the information system monitors and controls remote access methods
* Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions
* Ensure that the information system routes all remote accesses through managed network access control points to reduce the risk of external attacks
  1. **Wireless access**

The organisation shall:

* Establish usage restrictions, configuration/connection requirements and implementation guidance for wireless access
* Authorise wireless access to the information system prior to allowing such connections
* Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption
  1. **Access control for mobile devices**

The organisation shall:

* Establish usage restrictions, configuration requirements, connection requirements and implementation guidance for organisation-controlled mobile devices
* Authorise the connection of mobile devices to organisational information systems
* Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices
  1. **Publicly accessible content**

The organisation shall:

* Designate individuals authorised to post information onto a publicly accessible information system
* Train authorised individuals to ensure that publicly accessible information does not contain non-public information
* Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that non-public information is not included
* Review the content on the publicly accessible information system for non-public information regularly and remove such information if discovered to be out of date or incorrect
  1. **Monitoring user access**

Systems will be capable of logging events that have a relevance to potential breaches of security. User access will be subject to management checks.

# Responsibilities

* 1. **Senior Information Responsible Owner (SIRO)**

The SIRO is responsible for ensuring that the requirements of this policy are implemented within any programme, project, system or service for which they are responsible. A register of all IG roles/Responsible Persons should be made available (see [Annex C](#_Appendix_C_–)).

The SIRO is responsible for ensuring that a robust checking regime is in place and

complied with to ensure that legitimate user access is not abused.

The SIRO may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and the associated checking regime. Any non-compliance with this policy must be supported by a documented and evidence-based risk decision accepted by the SIRO.

* 1. **Managers**

Managers are responsible for ensuring that members of their team have the minimum levels of access to systems that they need to perform their job. They must authorise the access rights for each individual team member and keep a record of the latest access permissions authorised.

Managers should ensure that the access rights of people who have a change of duties or job role or have left the organisation are revoked immediately and that any access tokens (smartcard/USB dongle) are recovered. All managers should review the access levels of their people to ensure they are appropriate.

* 1. **Users**

Users must only use business systems for legitimate use as required by their job and in accordance with the procedures for those systems.

# Compliance

Compliance against this policy will be assessed regularly.

Breaches of this policy and/or security incidents can be defined as events which

could have, or have resulted in, loss or damage to the assets of this organisation or an event which is in breach of the organisation’s security procedures and policies.

All Grey Road Surgery employees, partners and directors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the organisation’s Information Governance Breach Reporting Policy. This obligation also extends to any external organisation contracted to support or access the information systems at this organisation.

The organisation will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee, the matter may be dealt with under disciplinary procedures.

# Annex A – Register of all IG roles/Responsible Persons

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Contact details** |
| **Caldicott Guardian** | Dr. Janet Bliss | Janet.bliss@livgp.nhs.uk |
| **Senior Information Risk Owner (SIRO)** | Dr.Catherine McNamara | Catherine.mcnamara2@nhs.uk |
| **Data Protection Officer (DPO)** | Head of Information Governance and Data Protection Officer  NHS Informatics Merseyside  Information Governance Team  Hollins Park  Winwick  Warrington  Cheshire  WA2 8WA | [DPO.IM@imerseyside.nhs.uk](mailto:DPO.IM@imerseyside.nhs.uk) |
| **Information Governance lead** | Angela Howgate | Angela.howgate@livgp@nhs.uk |
| **IT security lead** | Angela Howgate (for Practice)  Informatics Merseyside | Angela. Howgate@livgp@nhs.uk |

1. [↑](#footnote-ref-1)