**Staff Monitoring Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| 1.1 | June 2022 |  | AJH |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 2](#_Toc97712762)

[1.1 Guidance statement 2](#_Toc97712763)

[1.2 Status 2](#_Toc97712764)

[1.3 KLOE 2](#_Toc97712765)

[1.4 Training and support 2](#_Toc97712766)

[2 Scope 3](#_Toc97712767)

[2.1 Who it applies to 3](#_Toc97712768)

[2.2 Why and how it applies to them 3](#_Toc97712769)

[3 Guidance 3](#_Toc97712770)

[3.1 Monitoring electronic communications at work 3](#_Toc97712771)

[3.2 Accessing records of family and friends 4](#_Toc97712772)

[3.3 System security 5](#_Toc97712773)

[3.4 Recognised good practice for staff 5](#_Toc97712774)

[3.5 Staff declaration 6](#_Toc97712775)

[4 Training 6](#_Toc97712776)

# Introduction

## Guidance statement

This guidance for staff within Grey Road Surgery sets out the monitoring of work activity and the duties of confidence owed to its data.

## 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This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time.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 “Well-led.”

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)

## Why and how it applies to them

Grey Road Surgery and all appropriate staff are to ensure compliance with all requirements of this policy. Failure to comply with the policy and any associated [breaches](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/) of patient data or confidentiality could lead to prosecution or imposition of [penalties](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/) by the Information Commissioners Office (ICO).

# Guidance

All work activity on organisational systems and premises is monitored in accordance with the [Data Protection Act 2018](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiuyf7wz4n2AhUNi1wKHWcwDDEQFnoECAcQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2018%2F12%2Fcontents%2Fenacted&usg=AOvVaw1nLdFiC3yrsnW5qE79iLDw) and the [UK General Data Protection Regulation 2016](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj58LP-z4n2AhXPQkEAHVHfBmMQFnoECCwQAQ&url=https%3A%2F%2Fgdpr-info.eu%2F&usg=AOvVaw1akHzzz224Oq1yU0pd6qSw).

Monitoring in the workplace includes but is not limited to:

* Recording on CCTV cameras
* Opening mail or email
* Use of automated software to check email
* Checking phone logs or recording phone calls
* Checking logs of websites visited
* Videoing outside the workplace
* Collecting information through clinical systems to check the performance of individual staff

## Monitoring electronic communications at work

The organisation can legally monitor phone, internet or email use in the workplace if:

* + - The monitoring relates to the business
    - The equipment being monitored is provided partly or wholly for work
    - The organisation via this guidance has made all reasonable efforts to inform you that your communications will be monitored

Staff should bear in mind that these circumstances cover almost every situation where the organisation might want to monitor your electronic communications. Grey Road Surgery does not allow any system to be used for personal use at all.

The organisation does not need consent before monitoring electronic communications for any of these reasons:

* To establish facts which are relevant to the business, to check that procedures are being followed or to check standards – for example, listening to phone calls to assess the quality of work
* To prevent or detect crime
* To check for unauthorised use of telecommunications systems, such as whether an employee is using the internet or email for personal use
* To make sure electronic systems are operating effectively – for example, to prevent computer viruses entering the system
* To check whether a communication received, such as an email or phone call, is relevant to the business. The organisation can open your emails or listen to voicemails

## Accessing records of family and friends

Staff are able to access patient or staff records for business use only. This means for patients, the management of their healthcare and their healthcare needs, and if you have access to staff data, for employment purposes only. It is a breach of both the Data Protection legislation and common law duties of confidentiality to access any records for personal reasons.

This is especially important if you work in an organisation that has family members or friends as patients. Staff are not allowed (even with the person’s consent) to access family members’ records or friends’ records unless you are doing so for organisational purposes. It would always be recommended to ask a colleague, if possible, to deal with family or friends when they attend or contact the organisation but in the absence of the ability to do this, staff members must only access their record if they have a legitimate reason for doing so.

Being nosey to check up on family or friends or ‘just looking’ is a serious breach of law and contract of employment terms which could lead to both dismissal and criminal investigation against the staff member.

## System security

Staff members are not permitted to access any organisational system using another person’s login details and should never share passwords.

Accessing records using another person’s details is a breach of Data Protection law and the [Computer Misuse Act 1990](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi0_bbW0In2AhWRZMAKHXkhBFUQFnoECBIQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1990%2F18%2Fcontents&usg=AOvVaw1hrd6GOQftKy7ghGPjb-VU) which is again a serious breach of law and contract of employment terms which could lead to both dismissal and criminal investigation against the staff member.

## Recognised good practice for staff

* Safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation for everyone working on or behalf of NHS England.
* Clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
* Switch off computers with access to person-identifiable or business confidential information or put them into a password-protected mode if you leave your desk for any length of time.
* Ensure that you cannot be overheard when discussing confidential matters.
* Challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
* Share only the minimum information necessary.
* Transfer person-identifiable or confidential information securely, when necessary, i.e., use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g., gsi.gov.uk.
* Seek advice if you need to share patient/person-identifiable information without the patient/identifiable person’s consent and record the decision and any action taken.
* Report any actual or suspected breaches of confidentiality.
* Do not share passwords or leave them lying around for others to see.
* Do not share information without the consent of the person to whom the information relates unless there are statutory grounds to do so.
* Do not use person-identifiable information unless absolutely necessary, anonymise the information where possible.
* Do not collect, hold or process more information than you need and do not keep it for longer than necessary.

## Staff declaration

Principle 7 of the Data Protection Act 2018 requires organisations to protect information and data by appropriate security and accountability. Grey Road Surgery collects and stores information and data. To ensure the organisation meets data security requirements and compliance with Principle 7 of the Data Protection Act, it is vital to ensure that only those people with legitimate need are able to access the data this organisation holds.

Therefore, all new starters are required to sign a Staff Data Security Induction and Confidentiality Declaration to confirm that they accept their responsibilities in relation to Information Governance ([see Annex A](#_Appendix_A_–)).

# Training

Information Governance training is available on the GP TeamNet

# 

1. [Network DES specification](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjW_Mmq0vz1AhXCQEEAHXOHBpoQFnoECA4QAQ&url=https%3A%2F%2Fwww.england.nhs.uk%2Fpublication%2Fnetwork-contract-des-specification-2021-22%2F&usg=AOvVaw3xuhgNvg7oYsvX-M1E-Pns) [↑](#footnote-ref-1)