**Clear Desk and Clear Screen Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| v1.1 | 09/07/2024 | Sultan Mohamed | Nine Taylor |  |
|  | August 2025 |  |  | Next review |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 2](#_Toc141870437)

[1.1 Policy statement 2](#_Toc141870438)

[1.2 Status 2](#_Toc141870439)

[2 Requirement 2](#_Toc141870497)

[2.1 Background 2](#_Toc141870498)

[2.2 Objectives 3](#_Toc141870499)

[2.3 Key principles 3](#_Toc141870500)

[2.4 Definitions 4](#_Toc141870501)

[2.5 The Caldicott Principles 4](#_Toc141870502)

[2.6 Data Protection Act (2018) 5](#_Toc141870503)

[2.7 Disclosure 5](#_Toc141870504)

[3 Protecting confidential information 6](#_Toc141870505)

[3.1 Requirement 6](#_Toc141870506)

[3.2 Audit 9](#_Toc141870507)

[4 Legal framework 9](#_Toc141870508)

# Introduction

## Policy statement

This policy is to remind staff at Sheerwater Health Centre of their responsibility to maintain the confidence of all service users and how breaches may occur by a document being left on a desk, information on a PC monitor or simply data left in another area, be it within the practice or elsewhere.

Furthermore, the policy provides best practice guidance and should be read in conjunction with the following policies, procedures and guidance documents:

* [Data Protect Act 2018](https://www.gov.uk/data-protection)
* [Data Security and Protection Toolkit Handbook](https://practiceindex.co.uk/gp/forum/resources/data-security-and-protection-toolkit-handbook-pdf-version.1909/)
* [Governance handbook](https://practiceindex.co.uk/gp/forum/resources/the-governance-handbook.1817/)
* [UK GDPR Policy](https://practiceindex.co.uk/gp/forum/resources/uk-gdpr-policy.1703/)
* [Home-working policy and procedures](https://practiceindex.co.uk/gp/forum/resources/home-working-policy-and-procedures.842/)
* [Transportation of confidential records policy](https://practiceindex.co.uk/gp/forum/resources/transportation-of-confidential-records-policy.1378/)
* Other information governance policies that all support the completion of the Data Security Protection Toolkit.

All staff at this organisation are to be fully conversant with this policy and are to understand the requirement for effective controls of information governance.

## 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.legislation.gov.uk/ukpga/2010/15/contents). Consideration has been given to the impact this policy might have regarding 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. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

# Requirement

## Background

This document is intended to promote quality patient care through the proper use of information. Information is an asset to the organisation and needs to be suitably protected. All staff at this organisation are responsible for using and storing information appropriately.

The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation. Staff working for and on behalf of this organisation must also meet these legal requirements and may be bound by professional obligations, employment contracts or other contractual measures.

This organisation collects and stores information and data as a data controller. To ensure the organisation meets data security requirements and compliance with principle 7 (accountability) of the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted), it is vital to ensure that only those people with legitimate need are able to access the data this organisation holds.

This policy will ensure the organisation protects the information and data that is held, reducing the risk of information theft, fraud or a security breach caused by sensitive information being left unattended and visible in plain view. Any such incident must be reported via the Information Governance Breach Reporting process with the [Information Commissioner’s Office (ICO)](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/).

## Objectives

The objective of this policy is to protect information on patients and staff and also to be legally compliant with the Data Protection Act 2018 as well as the [NHS Code of Conduct on Confidentiality](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice).

The organisation may be vicariously liable for a negligent act or omission (e.g., the loss of personal data) if an employee is so closely connected with the performance of his or her employment that it would be fair to place the liability on the employer.

This organisation has a duty to inform its staff of the procedure or processes required to keep personal information secure and confidential.

The objective of this policy is to ensure that all paper and electronic media containing confid­ential or sensitive information (including person-identifiable information and corporate or com­mer­cial­ly sensitive information) is suitably secured when not in use and not left unattended or left visible on a desk overnight. This applies to working areas, such as desks, which should not have confidential, sensitive, commercially sensitive or person-identifiable information left on them when the information user is not present.

## Key principles

The aims of the policy are:

* To reduce the threat of a security breach or information theft
* To reduce the risk of confidential or sensitive information or documentation being stolen which could damage the integrity of this organisation
* To ensure compliance with the Data Protection Act 2018
* To create a culture of responsibility in relation to the handling and care of person-identifiable and other confidential information

## Definitions

1. **Personal information**

This is information about a living individual that can identify that person, e.g., name and private address, name and home telephone number, date of birth, National Insurance number, employee payroll number, NHS number.

1. **Sensitive personal information**

This is when the personal information contains details of that person’s:

* Health or physical condition
* Sexual life
* Ethnic origin
* Religious beliefs
* Political views
* Criminal convictions

For this type of information, even more stringent measures should be employed to ensure that the data remains secure.

The loss or disclosure of corporate/commercially sensitive information may reduce this organisation’s competitiveness or breach procurement practices, e.g., to building leases, commercial/third party contracts or internal plans.

## The Caldicott Principles

The Caldicott Principles require that all organisations having access to confidential information exercise good practice when dealing with confidential information for non-healthcare purposes:

* Justify the purpose(s) of using confidential information
* Only use it when absolutely necessary
* Use the minimum that is required
* Access should be on a strict need-to-know basis
* Everyone must understand his or her responsibilities
* Understand and comply with the law
* The duty to share information can be as important as the duty to protect patient confidentiality
* Inform patients and service users about how their confidential information is used

The Caldicott Guardian must approve any use of patient identifiable data for non-healthcare purposes.

Further reading can be sought from the **Caldicott and Confidentiality Policy.**

## Data Protection Act (2018)

The Data Protection Act (2018) governs the processing of personal data held on computer systems and in other formats. It imposes restrictions on how an individual’s data may be used.

Seven data protection principles must be applied when processing personal data:

* Processing personal data must be lawful, fair and transparent (i.e., the data subject is told who will be using his/her data and for what purpose)
* The purpose of processing personal data must be specified, explicit and legitimate
* Personal data must be adequate, relevant and not excessive
* Personal data shall be accurate and kept up to date
* Personal data shall not be kept for longer than necessary
* Personal data must be processed in a secure manner
* Accountability

In order to comply with the Data Protection Act (2018), this organisation has registered as a data controller and has notified the Information Commissioner of the purposes for which it processes personal data.

## Disclosure

Staff who wish to discuss issues of confidentiality should approach their line manager for assist­ance and advice on disclosure issues.

The following are also able to advise on issues regarding confidentiality:

|  |  |
| --- | --- |
| **Role** | **Name** |
| Practice Manager | Nine Taylor |
| Caldicott Guardian | Dr Munira Mohamed |
| SIRO | Dr Munira Mohamed |
| Information Governance Lead | Dr Munira Mohamed |
| Data Protection Officer | Dr Munira Mohamed / Nine Taylor |

# Protecting confidential information

## Requirement

Confidential or sensitive information, whether held electronically or on paper records, should be secured appropriately when people are absent from their workplace and at the end of each work­ing day.

The following principles cover both non-electronic (e.g., manual/paper files) as well as electronic forms of information. Reference is also made to the display of information on the computer/laptop screen as well as to the security of personal property.

1. **Working areas**

* Staff, clinicians and non-clinicians must not leave person/patient-identifiable information, personal files or any other confidential/sensitive records (including patient files, correspondence, minutes, reports and any other information which could be regarded as confidential or of a sensitive nature) unattended on their desks or around their work areas.
* Desks must be cleared of any confidential or person identifiable information at the end of each working day. Medical records/patient files must be locked securely in desks, filing cabinets or designated secure rooms at all times other than when they are being used by designated organisation staff.

All efforts must be made to keep information secure so that it is not readily accessible to non-authorised organisation staff.

* Person/patient identifiable information should be destroyed securely using approved methods of waste disposal. Documents containing personal or corporate sensitive information should never be put into a general waste bin.
* Personal items (e.g., keys, handbags, wallets) should be locked away safely in the interests of security. It is the responsibility of the owner to ensure security precautions are taken.

1. **Electronic data**

* For the purposes of this policy, electronic data and equipment are regarded as the same as manual records/equipment if they contain the same type of confidential, sensitive and/or personal information. Computing and other equipment containing data should be treated with the same level of security as paper-based resources.
* To ensure the security of information held electronically, lock away portable computing devices such as laptop computers or PDAs when not in use.
* To ensure the security of information held on ‘mass storage’ devices such as CD-ROM, DVDs or USB memory drives, lock these away in a secure drawer at the end of the working day.
* USB drives and other such items must be locked away even if they are encrypted.

1. **Information on computer screens**

* Computers and laptops must be locked when unattended by pressing the ‘Control, Alt, Del’ keys simultaneously then choosing ‘Lock computer’).
* Access to computers must be protected by password in line with the organisation’s **Confidentiality protocol -v3**
* If using a shared workstation, it is appropriate to log off rather than lock the computer. If an absence of more than 30 minutes is anticipated, the computer or laptop should be shutdown. This gives the benefit of power saving and also allows the completion of installs/updates that may have been deployed remotely and are awaiting a reboot and/or connection to the network.
* Monitors should also be turned off at the end of the working day.
* If sensitive or confidential information is being worked on, the screen must be closed, minimised or locked when unauthorised persons are in close proximity to the screen, if practical.
* If sensitive or confidential information is visible to an unauthorised person standing in close proximity to a computer/laptop screen, they should be asked to move away to protect the confidentiality of this information.
* Use the scan facility to make an electronic copy, save this to an appropriate secure network drive, saving to a folder that has the correct individual viewing permissions and destroy the hard copy if appropriate.

1. **Printers and photocopiers**

* It is the responsibility of the person who sends information to be printed to ensure he/she collects his/her documents rather than leave them unattended.

If information of a con­fidential/sensitive nature is misplaced or missing, this should be logged as an incident.

1. **Maintaining confidentiality outside the office**

* Staff should not discuss confidential information with friends or family.
* Paper records/information should be stored securely (not left on display at home or in a car).
* If working from home, the homeworker must carry out work for the organisation in a room that is private and confidential and must not allow members of their family or third parties who are not employed by the organisation to access or use the organisation’s equipment.
* The homeworker is responsible for keeping all documents and information associated with the organisation’s services and patients secure at all times. Confidential information should only be stored on home electronic media that is password-protected and has anti-virus software.

Specifically, homeworkers are under a duty to:

* Keep filing cabinets and drawers locked when they are not being used
* Keep all documentation belonging to the organisation under lock and key at all times except when in use
* Agree special arrangements for the disposal (shredding or otherwise) of confidential paper waste produced at home
* Be able to access Surgery Connect / EMIS / Docman / Accurx / Sheerwater Health centre emails / Shared drive and will take inbound and outbound telephone calls if required

It should be noted that under no circumstances will patient or personal identifiable information be permitted to be removed from the premises in any format without the express permission of the data controller.

## Audit

Information governance scheduled audit and unscheduled spot checks will take place on a regular basis to evaluate the effectiveness of training, identifying issues and weaknesses in order to manage and mitigate potential risk.

The findings will be documented and the information included in the DSP Toolkit annual submission.

# Legal framework

This organisation’s staff has a legal duty to comply with the following guidance which give the circumstances under which confidential information can be disclosed:

* [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=2ahUKEwiwg-PH5fz1AhUxQkEAHRX2DjwQFnoECA4QAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2018%2F12%2Fcontents%2Fenacted&usg=AOvVaw1nLdFiC3yrsnW5qE79iLDw)
* [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=2ahUKEwjtkovS5fz1AhVhoFwKHSnsCNkQFnoECAwQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1990%2F18%2Fcontents&usg=AOvVaw1hrd6GOQftKy7ghGPjb-VU)
* [The Health and Safety at Work Act (1974)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiE1ofa5fz1AhWPa8AKHVctAnsQFnoECAwQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1974%2F37%2Fcontents&usg=AOvVaw14VUyTl0-uN6DNmcZ_xe4m)
* [Human Rights Act (1998)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi2_e_i5fz1AhWVnVwKHcwmCaAQFnoECAwQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1998%2F42%2Fcontents&usg=AOvVaw1e5pKwsX2UgNYm4kE-Im1z)
* [Regulation of Investigatory Powers Act (2000)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiVosLr5fz1AhUNO8AKHc1sBtUQFnoECAkQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2000%2F23%2Fcontents&usg=AOvVaw34iK5TZfl3M_XLHn7aKzSx)
* [Freedom of Information Act (2000)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiv7Znz5fz1AhWSYMAKHXPPCWkQFnoECBAQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2000%2F36%2Fcontents&usg=AOvVaw2ED-_lceYVKNX9EF_BgWVI)
* [Health and Social Care Act (2008)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjB2MD75fz1AhUXgFwKHW0hDukQFnoECBAQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fid%2Fukpga%2F2008%2F14&usg=AOvVaw23UpPn3SpiJpcDTjYuIrUY)
* [The Caldicott Principles](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj03PmE5vz1AhWIiVwKHUbMCFQQFnoECA0QAQ&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fthe-caldicott-principles&usg=AOvVaw22orCuz9f5J5jLudjT1oIJ)
* [Confidentiality: NHS Code of Practice](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjw2_aT5vz1AhWGQkEAHbWpAcgQFnoECAwQAQ&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fconfidentiality-nhs-code-of-practice&usg=AOvVaw2hk75WSFduGdzUEdh-Ntem)