**Remote Access to IT Systems Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| v1 | 28/04/2020 | Sultan Mohamed |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 3](#_Toc37765621)

[1.1 Policy statement 3](#_Toc37765622)

[1.2 Status 3](#_Toc37765623)

[1.3 Training and support 3](#_Toc37765624)

[2 Scope 3](#_Toc37765625)

[2.1 Who it applies to 3](#_Toc37765626)

[2.2 Why and how it applies to them 3](#_Toc37765627)

[3 Definition of terms 4](#_Toc37765628)

[3.1 Remote access 4](#_Toc37765629)

[3.2 Remote working 4](#_Toc37765630)

[3.3 Portable device 4](#_Toc37765631)

[3.4 Microsoft Teams 4](#_Toc37765632)

[3.5 Zoom 4](#_Toc37765633)

[3.6 Clarity TeamNet 4](#_Toc37765634)

[3.7 Away From My Desk 4](#_Toc37765635)

[3.8 Advanced Network Monitoring 5](#_Toc37765636)

[3.9 CareCERT 5](#_Toc37765637)

[3.10 Cyber resilience 5](#_Toc37765638)

[3.11 Cyber security 5](#_Toc37765639)

[3.12 Clinical system 5](#_Toc37765640)

[3.13 Internet 5](#_Toc37765641)

[3.14 Intranet 5](#_Toc37765642)

[3.15 Health and Social Care Network 6](#_Toc37765643)

[4 Linked policies 6](#_Toc37765644)

[5 Security standards 6](#_Toc37765645)

[5.1 General guidance 6](#_Toc37765646)

[5.2 The ten standards 6](#_Toc37765647)

[5.3 Passwords 7](#_Toc37765648)

[5.4 Away From My Desk 8](#_Toc37765649)

[5.5 Microsoft Teams 8](#_Toc37765650)

[5.6 Video consultations 8](#_Toc37765651)

[5.7 Encryption and software 8](#_Toc37765652)

[6 Security essentials 8](#_Toc37765653)

[6.1 Mandatory actions 8](#_Toc37765654)

[7 Reporting the loss of a device and data 9](#_Toc37765655)

[7.1 Data breach 9](#_Toc37765656)

[7.2 Loss/theft of equipment 9](#_Toc37765657)

[8 Summary 9](#_Toc37765658)

[Annex A – Remote working security assessment 11](#_Toc37765659)

[Annex B – The Data Protection Impact Assessment 13](#_Toc37765660)

# Introduction

## Policy statement

The purpose of this policy is to ensure that all staff at Sheerwater Health Centre are fully aware of the precautions and security measures needed when accessing organisational IT systems remotely for the performance of their duties. This includes when staff are working from home on a regular or ad-hoc basis.

## 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. Consideration has been given to the impact this policy might have in 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.

## 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 of the organisation. Other individuals performing functions in relation to the organisation, such as agency workers, locums and contractors, are encouraged to use it.

## Why and how it applies to them

This document has been produced to provide all staff at Sheerwater Health Centre with the necessary level of information to understand remote access so that they are able to work safely and effectively in the performance of their daily duties.

# Definition of terms

## Remote access

The ability to access a computer or a network remotely through a network connection.

## Remote working

An arrangement permitting an employee to work from home either regularly or on an ad-hoc basis.

## Portable device

A portable device is any device that can easily be carried. Portable devices are primarily battery-powered devices with base computing resources in the form of a processor, memory, storage and network access, examples include tablets (i.e. iPads), laptops and smartphones.

## Microsoft Teams

Microsoft Teams is a unified communication and collaboration platform combining workplace chat, video meetings, files storage and application integration.

## Zoom

Zoom is a cloud-based platform for video and audio conferencing, chat and webinars.

## Clarity TeamNet

A web-based sharing and compliance platform for primary care.

## Away From My Desk

Away From My Desk (AFMD) is a remote access tool enabling employees to access their organisation’s computer remotely, replicating their workstation on their own device.

## Advanced Network Monitoring

The Advanced Network Monitoring (ANM) service inspects all internet traffic from Consumer Network Service Providers (CN-SPs) and instantly blocks any known malicious content.[[1]](#footnote-1)

## CareCERT

The Care Computer Emergency Response Team (CareCERT) provides advice and guidance to health and social care organisations to respond effectively and safely to cyber security threats.[[2]](#footnote-2)

## Cyber resilience

Although there is no standard definition, this can be referred to as an organisation’s ability to withstand or quickly recover from cyber events that disrupt usual business operations.[[3]](#footnote-3)

## Cyber security

Cyber security refers to the methods and processes used to protect electronic data.

## Clinical system

Clinical software systems such as EMIS Web, SystemOne or Vision used to record patient information.

## Internet

A global computer network providing a variety of information and communication facilities consisting of interconnected networks using standardised communication protocols[[4]](#footnote-4)

## Intranet

A system of connected computers that works like the internet and allows people within an organisation to communicate with each other and share information.2

## Health and Social Care Network

The Health and Social Care Network (HSCN) will provide a reliable, efficient and flexible way for health and care organisations to access and exchange electronic information.[[5]](#footnote-5)

# Linked policies

This policy is to be read in conjunction with the following PLUS policies:

* General Data Protection Regulation (GDPR) Policy
* Cyber Resilience Policy
* Communication Policy
* Intranet and Social Media Acceptable Use Policy
* Portable Device Policy
* Homeworking Policy and Procedure
* [insert other organisational policies as appropriate]

There may be NHS England (NHS(E)) and/or Clinical Commissioning Group (CCG) directives and/or policies that also compliment this policy.

# Security standards

## General guidance

All staff working remotely must ensure they adhere to the data security principles which are applied when working remotely for Sheerwater Health Centre. Also, when using any device, staff must ensure that information is not visible to other individuals, i.e. family members, who have no need to see the information.

Staff working remotely must complete the security assessment checklist at Annex A prior to working and a copy is to be forwarded to [insert name and role].

## The ten standards

The purpose of the ten standards is to enhance existing data security principles, thereby improving data security across the healthcare sector. The standards outline the value of safe, secure, appropriate and lawful data-sharing.3 Staff at Sheerwater Health Centre will adhere to the data security standards as outlined below.

The Data Security Standards are:[[6]](#footnote-6)

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Information Governance Toolkit.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses or which force staff to use workarounds which compromise data security.
6. Cyberattacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss with a report made to senior management within 12 hours of detection. Significant cyberattacks are to be reported to CareCERT immediately following detection.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report made to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian’s Data Security Standards.

## Passwords

In addition to system passwords, staff must set an access password for the device(s) they are using when working remotely. This password must be unique and not shared with anyone else. Passwords must contain a combination of:

* Upper-case letters
* Lower-case letters
* Numbers
* Non-alphabetical characters (\*&!@ etc.)

Passwords should be at least eight characters long and it is strongly recommended that passwords are changed regularly. If an organisational device becomes locked as a result of the incorrect password being inputted, support and/or password resets can be obtained from [insert relevant details here].

## Away From My Desk

At all times staff should use the Away From My Desk (AFMD) remote access tool and at no point should documents be downloaded and stored on their own or Sheerwater Health Centre devices.

## Microsoft Teams

Staff should use Microsoft Teams as directed by Sheerwater Health Centre predominantly for chat and also for file sharing where they are unable to utilise AFMD. In addition, any conference calls should take place using Zoom, supported and incorporated within Microsoft Teams.

## Video consultations

Clinical staff can undertake video consultations remotely using the [integrated] or [non-integrated] applications within [insert clinical system name].

## Encryption and software

All Sheerwater Health Centre portable devices must be encrypted with 256bit encryption and only approved software can be installed and used by staff. Further guidance can be found in the Portable Device Policy.

# Security essentials

## Mandatory actions

When working remotely staff must:

* Complete a security assessment checklist and forward it to [insert name and role]
* Use AFMD and Microsoft Teams
* Ensure they have a separate password/login for personal devices, i.e. shared home computers/tablets/smartphones
* Work in an area that is private and cannot be overlooked/overheard
* If this is not possible, filter screens should be applied and conversations restricted to ensure no patient identifiable information is discussed
* Ensure all practice related information is held securely, i.e. in a locked cabinet or drawer
* IT equipment is locked or logged out when not being used by the staff member
* Adopt a clear desk routine at all times
* Not print any practice related work at home
* Not work in high-risk areas, i.e. public places or on transport
* [organisation to add as deemed necessary]

# Reporting the loss of a device and data

## 7.1 Data breach

If there has been a data breach, this must be reported within 72 hours of being discovered. This can be done via the [Data Security and Protection Toolkit (DSPT)](https://www.dsptoolkit.nhs.uk/Incidents).

Incident reporting guidance is available from: <https://www.dsptoolkit.nhs.uk/Help/29>

If immediate advice and guidance related to a cyber security incident is required, contact the NHS Digital Data Security Centre on: 0300 303 5222.

## 7.2 Loss/theft of equipment

In the event of the theft of a device, the staff member must report this to the police and obtain a crime reference number.

Losses or thefts must also be reported to [insert name/role/contact details]. Further information is contained within the Portable Device Policy at Section 5.

# Data Protection Impact Assessment

## 8.1 Completing the assessment

When new systems are introduced, Sheerwater Health Centre will carry out a Data Protection Impact Assessment (DPIA), the template for which is at Annex B.

# Summary

Remote working enables staff to work from home on a regular or ad-hoc basis or as a result of the organisation business continuity plan coming into effect such as in the event of the loss of premises or a pandemic.

It is essential staff work in accordance with the guidance contained within this and the referenced policies thereby ensuring data security is at an optimal level at all times and patient information protected.

# Annex A – Remote working security assessment

|  |
| --- |
| **Premises** |
| Item | Yes | No | Comment |
| Is the building structurally sound, i.e. constructed of bricks and mortar?  |  |  |  |
| Is access to the building restricted? |  |  |  |
| Are doors and windows fitted with locks, including those that are easily accessible? |  |  |  |
| **Workstation** |
| Item | Yes | No | Comment |
| Is the workstation in an area that is private? |  |  |  |
| Can the workstation be overlooked? |  |  |  |
| Can the staff member be overheard when using the telephone or during video calls? |  |  |  |
| Can the screen/device be locked when leaving it unattended, even for short periods? |  |  |  |
| Do you have lockable storage facilities for portable devices, i.e. practice laptops/smartphones or tablets? |  |  |  |
| **IT security** |
| Item | Yes | No | Comment |
| Does the equipment have up to date antivirus software installed? |  |  |  |
| Have you installed remote access software on the device(s), i.e. AFMD, Teams etc.? |  |  |  |
| Have you completed all mandatory training relating to data security?  |  |  |  |
| Comments: Please add any additional comments below. |
|  |

|  |
| --- |
| To be completed by the employee: |
| Name |  | Job title |  |
| Signature |  |  |  |

|  |
| --- |
| To be completed by the manager: |
| Name |  | Job title |  |
| Security assessment acceptable | Yes:  | No: |
| Additional actions required: |
|  |
| Remedial actions taken acceptable | Yes: | No: |
| Additional comments: |
|  |
| Signed: |  |
| Date: |  |
| Review date: |  |

# Annex B – The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at [organisation].

**Step 1 – Determining the need**

|  |  |  |
| --- | --- | --- |
| Does the process involve any of the following: | Yes | N0 |
| The collection, use or sharing of existing data subjects’ health information? |  |  |
| The collection, use or sharing of additional data subjects’ health information? |  |  |
| The use of existing health information for a new purpose? |  |  |
| The sharing of data subjects’ health information between organisations? |  |  |
| The linking or matching of data subjects’ health information which is already held? |  |  |
| The creation of a database or register which contains data subjects’ health information? |  |  |
| The sharing of data subjects’ health information for the purpose of research or studies (regardless of whether the information is anonymised)? |  |  |
| The introduction of new practice policies and protocols relating to the use of data subjects’ personal information? |  |  |
| The introduction of new technology in relation to the use of data subjects’ personal information, i.e. new IT systems, phone lines, online access, etc? | ✓ |  |
| Any other process involving data subjects’ health information which presents a risk to their “rights and freedoms”? |  |  |

**If the answer is yes to one or more of the above questions, a DPIA is required. Proceed to Step 2.**

**Step 2 – Assessing the risks**

|  |
| --- |
| **Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject** |
| What information is being collected and how? |  |
| Where is the information being collected from and why? |  |
| How often is the information being collected? |  |
| **Information use – Is the data obtained for specified, explicit and legitimate purposes?** |
| What is the purpose of using the information? |  |
| When and how will the information be processed? |  |
| Is the use of the information linked to the reason(s) for the information being collected? |  |
| **Information attributes – Personal data shall be accurate and, where necessary, kept up to date** |
| What is the process for ensuring the accuracy of data? |  |
| What are the consequences if data is inaccurate? |  |
| How will processes ensure that only extant data will be disclosed? |  |
| **Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** |
| What security processes are in place to protect the data? | * AFMD, Microsoft Teams, Clarity TeamNet and Zoom are approved by NHS(E) for use
* Portable devices are encrypted with 256bit encryption
* All staff have completed Data Security Awareness Training
* [Organisation] has completed the DSP Toolkit
* All staff have read the policies outlined at Section 4
* Remote systems include two-factor authentication
 |
| What controls are in place to safeguard only authorised access to the data? | * EMIS/SystmOne/Vision only accessed by AFMD
* EMIS/ SystmOne/Vision accessed using a Token with two-factor authentication
* All staff have individual logins for system access
* Control measures outlined in this policy as well as those policies outlined at Section 4
* No data is download onto personal or portable devices
* No data is printed remotely
 |
| How is data transferred. Is the process safe and effective? | * Staff access data using only approved software, i.e. AFMD, Microsoft Teams and Clarity TeamNet.
* Clinical information can only be shared on EMIS/SystmOne/Vision
 |
| **Data subject access – Personal data shall be accurate and, where necessary, kept up to date** |
| What processes are in place for data subject access? |  |
| How can data subjects verify the lawfulness of the processing of data held about them? |  |
| How do data subjects request that inaccuracies are rectified? |  |
| **Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures** |
| Will information be shared outside the organisation? Are data subjects made aware of this? |  |
| Why will this information be shared? Is this explained to data subjects? |  |
| Are there robust procedures in place for third-party requests which prevent unauthorised access? |  |
| **Retention of data – Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed** |
| What are the retention periods associated with the data? |  |
| What is the disposal process and how is this done in a secure manner? |  |
| Where is data stored? If data is moved off-site, what is the process? How can data security be assured? |  |

**Continued overleaf...**

**Step 3 – Risk mitigation**

|  |
| --- |
| **Information collection – The risk** |
| Personal data is collected without reason or purpose – increased risk of disclosure. |
| **Information collection – The mitigation** |
| The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected. |
| **Information use – The risk** |
| Personal data is used for reasons not explained to, or expected by, the data subjects.  |
| **Information use – The mitigation** |
| Clearly explain and display to data subjects how their information will be used.  Data-sharing requires a positive action, i.e. opting in, not opting out! |
| **Information attributes – The risk** |
| Data is inaccurate or not related to the data subject. |
| **Information attributes – The mitigation** |
| Make sure robust procedures are in place to ensure the data held about data subjects is accurate, up to date and reflects the requirements of the data subject for which it was intended. |
| **Information security – The risk** |
| Unauthorised access to data due to a lack of effective controls or lapses of security/procedure. |
| **Information security – The mitigation** |
| Ensure that staff are aware of the requirement to adhere to the organisation’s security protocols and policies; conduct training to enhance current controls. |
| **Data subject access – The risk** |
| Data subjects are unable to access information held about them or to determine if it is being processed lawfully. |
| **Data subject access – The mitigation** |
| Ensure that data subjects are aware of access to online services and know the procedure to request that information held be amended to correct any inaccuracies.  |
| **Information disclosure – The risk** |
| Redacting information before disclosure might not prevent data subjects being identified – i.e. reference to the data subject may be made within the details of a consultation or referral letter. |
| **Information disclosure – The mitigation** |
| Make sure the policy for disclosure is robust enough to ensure that identifying information is removed. |
| **Retention of data – The risk** |
| Data is retained longer than required or the correct disposal process is not adhered to. |
| **Retention of data – The mitigation** |
| Ensure that organisation policies and protocols clearly stipulate data retention periods and disposal processes. Review and update protocols and policies and, if necessary, provide training for staff to ensure compliance. |

1. [NHS Digital Cyber Security](https://digital.nhs.uk/services/health-and-social-care-network/new-to-hscn/improving-cyber-security) [↑](#footnote-ref-1)
2. [DoH CareCERT](https://www.igt.hscic.gov.uk/CyberWhatIs.aspx) [↑](#footnote-ref-2)
3. [Bitsight Cybersecurity Vs Cyber Resilience](https://www.bitsighttech.com/blog/cyber-resilience) [↑](#footnote-ref-3)
4. [Cambridge Dictionary](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwiFoPnUs77aAhVLJMAKHXNgCOMQFghJMAI&url=https%3A%2F%2Fdictionary.cambridge.org%2Fdictionary%2Fenglish%2Fthe-internet&usg=AOvVaw31S4n11frcvwNHaA-Emckq) [↑](#footnote-ref-4)
5. [NHS Digital](https://digital.nhs.uk/services/health-and-social-care-network) [↑](#footnote-ref-5)
6. [DoH Your Data: Better Security, Better Choice, Better Care](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf) [↑](#footnote-ref-6)