**Cyber Resilience Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
|  | 26.09.23 | M Pedlow |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 3](#_Toc135808581)

[1.1 Policy statement 3](#_Toc135808582)

[1.2 Status 3](#_Toc135808583)

[2 Resilience 4](#_Toc135808584)

[2.1 Improving cyber security 4](#_Toc135808585)

[2.2 Enhanced protection 4](#_Toc135808586)

[2.3 Improved protection and resolution 4](#_Toc135808587)

[2.4 NHS Digital Security Centre 4](#_Toc135808588)

[3 Data security standards 4](#_Toc135808589)

[3.1 The 10 standards 4](#_Toc135808590)

[3.2 Data Security and Protection Toolkit (DSPT) 6](#_Toc135808591)

[4 Precautionary measures 6](#_Toc135808592)

[4.1 Appointments 6](#_Toc135808593)

[4.2 Finance 6](#_Toc135808594)

[4.3 Communication 7](#_Toc135808595)

[4.4 Site sharing 7](#_Toc135808596)

[5 Response 8](#_Toc135808597)

[5.1 Liaison 8](#_Toc135808598)

[5.2 NHS Digital Data Security Centre 8](#_Toc135808599)

[5.3 Remaining on-site 8](#_Toc135808600)

[5.4 Transfer of care 8](#_Toc135808601)

[6 Recovery 8](#_Toc135808602)

[6.1 Appointments and administration 8](#_Toc135808603)

[6.2 Finance 9](#_Toc135808604)

[6.3 Communication 9](#_Toc135808605)

[7 Summary 9](#_Toc135808606)

[Annex A – Incident management pro forma 10](#_Toc135808607)

# Introduction

## Policy statement

Cyber threats are constantly evolving and always present and, increasingly, digital health organisations must remain prepared and ready to respond. Cyber resilience enables The Green Medical Centre to operate effectively by detecting, responding to and recovering from cyber-attacks which have the potential to impact on service delivery and patient care.

It is the responsibility of all staff to ensure that they use the organisation’s IT assets appropriately and in accordance with the following policies:

* [Audio Visual and Photography Policy](https://practiceindex.co.uk/gp/forum/resources/1517)
* [CareSnap Policy](https://practiceindex.co.uk/gp/forum/resources/1055)
* [Communication Policy](https://practiceindex.co.uk/gp/forum/resources/1008)
* [Cookie Policy](https://practiceindex.co.uk/gp/forum/resources/1580)
* [Data Security and Protection Toolkit Handbook](https://practiceindex.co.uk/gp/forum/resources/data-security-and-protection-toolkit-handbook-ms-word-version.1908/)
* [GP Mythbuster 85: Data security and protection – expectations for general practice](https://www.cqc.org.uk/guidance-providers/gps/nigels-surgery-85-data-security-protection-expectations-general-practice)
* [Home Working Policy and Procedures](https://practiceindex.co.uk/gp/forum/resources/842)
* [Information sharing agreement](https://practiceindex.co.uk/gp/forum/resources/1022)
* [Intranet and Social Media Acceptable Use Policy](https://practiceindex.co.uk/gp/forum/resources/1001)
* [Portable Device Policy](https://practiceindex.co.uk/gp/forum/resources/967)
* [Smartcard Policy](https://practiceindex.co.uk/gp/forum/resources/1110)

This document will illustrate the organisation’s commitment to the safety of patient information. By adhering to the referenced guidance, staff will ensure that data and information is protected which will reduce the risk of cyber incidents in the future.

Further information, support and tools are available from: [NHS Digital Cyber and data security.](https://digital.nhs.uk/cyber)

Please note that at the time of writing (May 2023), NHS England and NHS Digital have merged. However, they remain as two separate sites on the internet.

## 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.

# Resilience

## Improving cyber security

The [Health and Social Care Network](https://digital.nhs.uk/services/health-and-social-care-network) (HSCN) has extensive security monitoring and analysis capabilities which enhance network security at The Green Medical Centre However, [NHS Digital](https://digital.nhs.uk/services/health-and-social-care-network/improving-cyber-security) states that the HSCN should not be considered a secure network and all connected organisations must risk assess their use of the HSCN and employ their own security controls to protect any data for which they are responsible. The HSCN will not automatically encrypt any data or guarantee the security of data or communications by default.

## Enhanced protection

[NHS Secure Boundary](https://digital.nhs.uk/cyber-and-data-security/managing-security/nhs-secure-boundary) provides a security solution that offers protection against the most sophisticated network security threats for NHS organisations. NHS Secure Boundary uses next generation firewall (NGFW) and web application firewall (WAF) protection to protect internet traffic from digital and cloud-based threats.

## Improved protection and resolution

The HSCN Network Analytics Service (NAS) monitors the heartbeat of the HSCN and identifies any new or anomalous behaviour on any part of the HSCN. The NAS was specifically designed to counter the rising threat from encrypted traffic. The NAS will benefit from early warning information sources such as the [National Cyber Security Centre (NCSC).](https://www.ncsc.gov.uk/) The NHS Secure Boundary service and the Domain Naming Servers (DNS) interface with the DNS being provided by the NCSC which blocks bad websites in real time preventing people from accessing them.

## NHS Digital Security Centre

The NHS Digital Data Security Centre will contact HSCN users if malicious activity or malware is detected by the HSCN. The aim is to help to resolve cyber security incidents and, where needed, help The Green Medical Centre] to prevent further incidents or disruption.

# Data security standards

## The 10 standards

The purpose of the 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.Staff at The Green Medical Centre will adhere to the [National Data Guardian’s (NDG) 10 data security standards](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides) as outlined below.

The data security standards are:

1. Personal confidential data – 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.

Further detailed information on providing evidence of achieving Standard 1 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-1-personal-confidential-data).

1. Staff responsibilities – All staff understand their responsibilities under the NDG’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

 Further detailed information on providing evidence of achieving Standard 2 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-2---staff-responsibilities).

1. Staff training – All staff complete appropriate annual data security training and pass a mandatory test, through appropriate training mechanisms.

 Further detailed information on providing evidence of achieving Standard 3 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-3---staff-training).

1. Managing data access – 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.

 Further detailed information on providing evidence of achieving Standard 4 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-4-managing-data-access).

1. Process reviews – 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.

 Further detailed information on providing evidence of achieving Standard 5 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-5---processes).

1. Responding to incidents – 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.

Further detailed information on providing evidence of achieving Standard 6 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-6---responding-to-incidents).

1. Continuity planning – 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 to senior management.

 Further detailed information on providing evidence of achieving Standard 7 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-7-continuity-planning).

1. Unsupported systems – No unsupported operating systems, software or internet browsers are used within the IT estate.

 Further detailed information on providing evidence of achieving Standard 8 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-8-unsupported-systems).

1. IT protection – 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.

 Further detailed information on providing evidence of achieving Standard 9 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-9---it-protection).

1. Accountable suppliers – IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the NDG’s Data Security Standards.

 Further detailed information on providing evidence of achieving Standard 10 is available [here](https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-10---accountable-suppliers).

## Data Security and Protection Toolkit (DSPT)

The [DSPT](https://www.dsptoolkit.nhs.uk/) is an online self-assessment tool that allows organisations to measure their performance against the NDG’s 10 data security standards. All organisations that have access to patient data are required to use the toolkit for assurance purposes and to ensure personal information is being correctly managed. Completion of the DSPT self-assessment is an annual requirement with assessments usually to be submitted by the 31 March each year.

Further supporting tools and information is available from the organisation’s [Data Security and Protection Toolkit handbook](https://practiceindex.co.uk/gp/forum/resources/data-security-and-protection-toolkit-handbook-pdf-version.1909/).

# Precautionary measures

## Appointments

On a daily basis, the individual responsible for opening the practice that day will be required to print off the appointment schedule for the day. This includes all clinical appointments and home visits.

Should home visit lists not be compiled until later in the morning session, whoever is responsible for ensuring that the home visit lists are printed and stored securely until required by the clinician.

## Finance

The Business Manager is responsible for all financial matters at The Green Medical Centre Should an attack occur, they will liaise with Lloyds Bankand Regency to advise them of the attack in order to protect the organisation’s finances and to ensure that staff are paid on time if the attack was to occur when payment is due.

## Communication

The table below illustrates the contact cascade should a cyber-attack occur at The Green Medical Centre

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Contact number(s) | Informing |
| Mike Pedlow | Business manager | Home:Mobile:  | Lynne Manning |
| Lynne Manning | Admin Manager | Home:Mobile: | Rest of staff |

Depending on the severity of the incident, the practice manager will also inform the following:

NWLICB

Hillingdon Federation

PCN neighbouring practices

Winchester pharmacy

The severity of the incident will define the requirement to communicate the attack externally. In the event of a prolonged IT outage, Mike Pedlow will liaise with NWL ICB to arrange a press release to raise awareness within the local community.

## Site sharing

In the event of an incident affecting the operability of it has been agreed locally that a reduced service will operate from The decision to close The Green Medical Centre and transfer services to Otterfield Medical Centre will depend on the severity of the incident the organisation faces.

Additionally, Otterfield Medical Centre will use this practice should its practice be affected by an incident. This is reflected in the [business continuity plans](https://practiceindex.co.uk/gp/forum/resources/business-continuity-policy.1056/) of both The Green Medical Centre and Otterfield Medical Centre

The contact details for [are:

Practice manager – Dr Fahad

Telephone number – request MP

# Response

## Liaison

The members of the practice management team at The Green Medical Centre are required to meet to discuss business output. Once the estimated outage time frame has been established, the Business Manager will liaise with Tarvinder Talsi of the ICB and advise them of the issue. The incident management pro forma at Annex A can be used as a guide to ensure the effective management of an incident.

## NHS Digital Data Security Centre

The Business Manager will report all cyber attacks to NHS Digital’s Data Security Centre on 0300 303 522. For general data security centre queries, email carecert@nhsdigital.nhs.uk.

## Remaining on-site

The practice management team may opt to remain on-site at The Green Medical Centre and continue to provide limited services to the patient population using paper forms and handwritten prescriptions. This decision will depend on factors such as the estimated time of the outage, local arrangements with pharmacies and the available facilities at the alternative practice.

# Recovery

## Appointments and administration

The recovery phase will be determined by the length of the outage. Appointments will have to be managed in a controlled and effectual manner. There will be a requirement to liaise with Otterfield Medical Centre to facilitate the transfer of information for those patients seen at that site, and to ensure that any laboratory results etc. are transferred to in a timely manner.

## Communication

The Business Manageris required to inform the following organisations once IT services have been restored:

* NWL ICB
* Winchester pharmacy

PCN

Furthermore, the Business Manager is to liaise with Tarvinder Talsi at ICB to discuss a press release to raise awareness among the patient population that normal services have been resumed and how appointments are being controlled.

# Summary

It is inevitable that The Green Medical Centre will at some point be affected by an incident that is out of their control. Such incidents will require effective, timely management if the expected level of service is to be provided to the entitled patient population. Ensuring that staff understand the potential impact and exercising the scenarios with staff will enable the team at The Green Medical Centre to manage situations effectively and minimise the disruption until normal services are resumed.

# Annex A – Incident management pro forma

|  |  |  |  |
| --- | --- | --- | --- |
| Date: |  | Time: |  |
| Person reporting incident: |  | Role: |  |
| Overview of incident: |  |
| Services affected: |  |
| Cause (if known): |  |
| Incident level: |  | Recovery time frame: |  |
| Emergency services required (yes or no) and state which services required: |  | Time called:Time arrived: |  |
| Evacuation necessary (yes or no): |  | All personnel accounted for (time achieved): |  |
| Key safety implications (yes or no): |  | Information passed to relevant authorities:Time achieved: |  |
| Cascade required (yes or no): |  | Escalation required (yes or no): |  |
| Time cascade complete: |  | Time escalation made: |  |
| Site share required (yes or no): |  | [Insert practice name] contacted and advised: |  |
| Determine available space at site share and decide what resources will be sent to that site: |  |
| If site share not required, determine which areas are affected and which are operable: |  |
| Review service provision in line with above: |  |
| Communication – Advise internal and external stakeholders appropriately: |  | Time achieved: |  |
| Health & Safety implications: |  |
| External agencies that need to be involved as a result of any H&S implications: |  |
| If applicable, inform the landlord/building owner: |  | Time notified: |  |
| Is patient confidentiality compromised (yes, no, maybe): |  | How is it compromised: |  |
| Impact of confidentiality breach: |  | Actions to reduce impact: |  |
| Date & time pro forma completed: |  | Review required (yes or no): |  |
| Planned review date & time: |  | Outcome (incident over or ongoing): |  |
| Additional review (if necessary): |  | Date & time incident ended and services resumed: |  |
| Practice manager signature:  |  | Name: |  |
| Senior partner signature: |  | Name: |  |