Sherwood Forest Hospitals
NHS Foundation Trust

TITLE: PASSWORD MANAGEMENT PROCEDURE

Document Category:	**INFORMATION GOVERNANCE**
Document Type:	**PROCEDURE**

Keywords:	Information security

Version:	**Issue Date:**	**Review Date:**
2.0	July 2024	January 2026

Supersedes:	1.0		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	19th March 2024

Scope/ Target Audience: (delete as applicable and/ or describe)	**Trust-wide**

Evidence Base/ References:	UK General Data Protection Regulation National Cyber Security Centre

Lead Division:	Corporate
Lead Specialty/ Department: (Or Division if 'divisionally' owned)	Information Governance
Lead Author: (position/ role and name)	Gina Robinson, Data Security and Privacy Compliance Officer
Co-Author(s): (position/ role and name if applicable)	
Sponsor (position/ role):	Jacquie Widdowson, Head of Data Security and Privacy and Data Protection Officer

Name the documents here or record not applicable	
(these are documents which are usually developed or reviewed/ amended at the same time – ie a family of documents)	
Associated Policy	Information Security
Associated Guideline(s)	
Associated Pathway(s)	
Associated Standard Operating Procedure(s)	Information Asset Owner Framework
Other associated documents e.g. documentation/ forms	

Consultation Undertaken:	• Information Governance Working Group

Template control:	v2.0 September 2023

Amendments from previous version(s)

Version	Issue Date	Section(s) involved (author to record section number/ page)	Amendment (author to summarise)
2	July 2024	Whole document – planned review undertaken	• No changes in practice • Evidence base updated

CONTENTS

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact sfh-tr.information.governance@nhs.net.

1 INTRODUCTION/ BACKGROUND

Passwords are an important aspect of data security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Trust's network. As such, all staff with access to Trust systems are responsible for taking the appropriate steps, as outlined below, to select, use and secure their passwords.

2 AIMS/ OBJECTIVES/ PURPOSE (including Related Trust Documents)

The purpose of this procedure is to raise awareness of the importance for the creation of strong passwords, the protection of those passwords, and the frequency of password change across all systems.

Attackers use a variety of techniques to discover passwords, exploiting a range of social and technical vulnerabilities.

These include:

- tricking someone into revealing their password via social engineering (including phishing and coercion)
- using the passwords leaked from data breaches to attack other systems where users have used the same password
- password spraying (using a small number of commonly used passwords to access many accounts)
- brute-force attacks (the automated guessing of large numbers of passwords until the correct one is found)
- theft of a password hash file, where the hash can be broken to recover the original passwords
- 'shoulder surfing' (observing someone typing in their password)
- finding passwords which have been stored insecurely, such as sticky notes kept close to a device, or documents stored on devices
- manual password guessing (using personal information 'cribs' such as name, date of birth, or pet names)
- intercepting a password (or password hash) as it is transmitted over a network
- installing a keylogger to intercept passwords when they are entered into a device.

These techniques are widely available and documented on the internet, and many use automated tools requiring only moderate technical skills.

All IT systems should require users to have an individual username and password. Your password is your main protection against someone else using your account. The password is used to confirm the identity of the person using the system as the authorised user and acts as a barrier against someone else accessing unauthorised information.

It is important that every employee takes seriously, the use, protection, and integrity of their own password/s or any other system password/s which they may be privy to from time to time and to encourage, guide and inform staff wherever possible for those who are responsible for the supervision of others.

Related Trust Documents

- Information Security Policy
- Information Asset Owner Framework
- Account Management and Access Policy
- Account Management Standard Operating Procedure

3 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has overall responsibility for this procedure within the Trust. Implementation of, and compliance with this procedure is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner (SIRO)

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer

We are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Director of Corporate Affairs and works with the Caldicott Guardian.

The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and considers the nature, scope, context, and purposes of processing.

Information Asset Owners

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they can understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators
Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents, and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

All Staff
All staff (including Medirest, Skanska, agency, and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for Data Protection and confidentiality.

Contractors and agency staff and other third parties' staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of IG security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors. Any IG security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team sfh-tr.information.governance@nhs.net.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read, and understood our data protection and confidentiality policy and accept their personal responsibility to always maintain confidentiality. Template confidentiality agreements for individuals/multiple individuals are available from the IG team.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our policy and accept their personal responsibility to always maintain confidentiality.

4 PROCEDURE DETAILS (including Flowcharts)

4.1 How to avoid choosing obvious passwords

The National Cyber Security Centre recommends that passwords should be three random words[1]. For example, CloudPenBag20 or CloudPenBag20!

Passwords must not be anything someone else could easily guess such as the names of your partner, children or pets, or your favourite holiday destination.

Passwords must not be based on easily accessible or discoverable information i.e., information recorded on personal social media accounts.

You could pick three things you can see around you or three words about your favourite book, music group, sport, film, hobby, or even a memorable day, though we would not recommend using your wedding day. **The three random words could be about anything, make sure they are easy for you to remember but hard for anyone else to guess.**

4.2 How to choose a strong password

Choosing a password that is 'strong' will help to ensure that information is kept safe and secure.

Try to create passwords that can be easily remembered. You could choose a song and use the first letter from each word to form your password Eg 'If you are happy and you know it clap your hands' could become **Iyhaykicyh!!** You could even replace the 'I' with a '1' and the 'a' with a '&' **1yh&yk1cyh!!** Strong passwords have the following characteristics:

- Contain both upper- and lower-case letters (e.g., a-z, A-Z)
- Contain numbers and punctuation characters in addition to letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./
- Must be at least eight alphanumeric (combination of alphabetical and numerical characters) long.

A strong password should not:

- Spell a single word.
- Spell a word with a number added to the beginning and/or the end.
- Be based on any personal information such as user id, family name, pet, birthday, etc.

Check your password strength: **Password Check | Kaspersky[2]**

4.3 Do not use common passwords

You must not use the following personal details for your password:

χ Current partner's name

[1] https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words
[2] https://password.kaspersky.com

- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team.

Below is a link to the top 100,000 passwords, these must not be used. https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt.

4.4 Can I write my password down?

Yes, some passwords can be written down but **must not** be stored with the account it relates to i.e., a word document with username and passwords must not be stored on a pc/laptop where you access systems or a smartcard with the pin number attached to it. Please note: if you can memorise passwords for key systems i.e., Windows, CareFlow, ESR, do not record them anywhere. If you have elevated access to key systems that contain confidential information or systems that are used to protect our IT infrastructure these **must not** be written down.

4.5 Responsibilities of super users/system administrators?

- ensuring an effective movers/leavers process is in place
- automatically locking out inactive accounts
- monitoring logins for suspicious behaviour (such as unusual login times, logins using new devices)
- encouraging users to report when something is suspicious

A record of staff having elevated, or administrator access rights will need to be maintained by the Information Asset Owner/Administrator.

Access will need to be regularly reviewed and revoked where applicable. An effective movers/leavers process should be in place.

Event logs will need to be protected against tampering (i.e. read only) if system access will be required to be monitored.

4.6 Managing shared access

Many accounts will have a way to **delegate** privileges to another account (such as access to a document or inbox).

4.7 Have different passwords for work and personal use

Do not use the same passwords for work and personal use i.e., online banking, online shopping, email accounts.

4.8 Changing Passwords

Passwords should be changed regularly, and you **should not** reuse your passwords. Even if a system allows, avoid reusing a password. Reusing that password could allow someone unauthorised access to your account.

Mandatory password changes may be forced on key systems according to the password policy set by the Trust e.g Windows. Changing passwords regularly helps to prevent misuse of your account without your knowledge if your password was somehow accidentally (or deliberately) disclosed.

You can change your password as often as you like or if you think it has been compromised. Contact the NHIS Service Desk (01623 410310 or x4040) to find out how you can change your Windows and other passwords.

Unlock a Windows Account NHIS Customer Portal (notts-his.nhs.uk).

4.9 What do I do if someone knows my password?

Log as an incident on the Trust's incident reporting system Datix, change your password(s) immediately and inform NHIS ServiceDesk as soon as possible.

4.10 Password Managers

When you are logging into your online accounts, for example social media, most web browsers (such as Chrome, Safari, and Edge) will offer to save them for you. It is safe for you to do this on your own device at home for example, but you must not do this on a Trust issued device.

Saving passwords on shared computers

The Trust has several shared devices, and there have been incidents where employees have been able to log into other colleagues accounts due to the previous employee not logging off.

If you are using a shared computer outside your home (for instance, at work, a college or library) you must never save your password in a browser.

4.11 What you must do

- ✓ Staff are responsible for keeping their login credentials secure (this includes Smartcards), and must ensure it is neither disclosed to, nor used by anyone else, under any circumstances.

- ✓ Staff must only access systems using their own username and password.

- ✓ Use different passwords for different systems - this helps to prevent unauthorised persons from gaining access to your other accounts and data on other systems if your password is compromised on one system.

- ✓ Always keep passwords secret and protected.

- ✓ Change your password regularly.

- ✓ All staff are accountable for any activity carried out under their login (username) and password, and this is audited.

- ✓ Change your password immediately if you suspect someone knows it. The suspected compromise should also be reported immediately as a security incident.

- ✓ Staff must ensure any unattended devices are logged out of or locked securely.

4.11 What you must not do

- ✗ Do not use the same password for work and personal/home systems.

- ✗ Avoid using the same password for multiple accounts. While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems.

- ✗ Do not share your password with anyone for any reason, including your manager, IT department staff or security staff.

- ✗ Do not use automatic logon (such as 'remember me') functionality, particularly if you are using a shared workstation or laptop. Using automatic logon functionality negates much of the value of using a password. If a malicious user can gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

5	EDUCATION AND TRAINING

Training

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff

must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[3] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation

A copy of this procedure and all related policies and procedures are provided to all staff and patients on the Trust's website.[4]

6 MONITORING COMPLIANCE AND EFFECTIVENESS

Legislative Changes will be monitored by the Head of Data Security and Privacy and reported bi-monthly to the Information Governance Committee.

7 EQUALITY IMPACT ASSESSMENT (please complete all sections of form)

- Guidance on how to complete an Equality Impact Assessment
- Sample completed form

Name of service/policy/procedure being reviewed:			
New or existing service/policy/procedure:			
Date of Assessment:			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?	b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?	c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality
The area of policy or its implementation being assessed:			
Race and Ethnicity:	None	Not applicable	None

[3] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[4] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/

Gender:	None	Not applicable	None
Age:	None	Not applicable	None
Religion / Belief:	None	Not applicable	None
Disability:	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality:	None	Not applicable	None
Pregnancy and Maternity:	None	Not applicable	None
Gender Reassignment:	None	Not applicable	None
Marriage and Civil Partnership:	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation):	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None, however, this procedure has been reviewed by the Information Governance Working Group.

What data or information did you use in support of this EqIA?

- Trust guidance for completion of the Equality Impact Assessments.

As far as you are aware are there any Human Rights issues be considered such as arising from surveys, questionnaires, comments, concerns, complaints, or compliments?

- No.

Level of impact

From the information provided above and following EqIA guidance document please indicate the perceived level of impact:

Low Level of Impact.

Name of Responsible Person undertaking this assessment:

Signature: G.H.Robinson

Date: 16th November 2023

8 APPENDICES