THE STATE HOSPITALS BOARD FOR SCOTLAND

PASSWORD POLICY

Policy Reference Number	IG25
Issue Number	2
Lead Author	Infrastructure Operations & IT Security Manager
Contributing Author(s)	Head of eHealth Information Security and Data Protection Officer Senior Information Risk Owner Caldicott Guardian
Advisory Group	eHealth Sub-Group
Approved By	Policy Approval Group (PAG)
Implementation Date	25 June 2025
Next Review Date	25 June 2028
Accountable Executive Director	Director of Finance and eHealth

The date for review detailed on the front of all State Hospital policies, procedures and guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy, procedure and guidance at any time due to organisational or legal changes.

Staff are advised to always check that they are using the correct version of any policy, procedure or guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies, procedures and guidance can be found on the Hospital's Intranet policies page.

REVIEW SUMMARY SHEET

Changes required to policy (evidence base checked) **Yes** ☐ **No** ☒

CONTENTS

1 INTRODUCTION / PURPOSE

The purpose of this policy is to outline the acceptable use and behaviour of all State Hospital Boards for Scotland (TSH) staff and their use of passwords. This includes passwords that will either be provided to support them in undertaking their role and fulfilling their duties and responsibilities or be configured by TSH staff for accessing systems used within\for their role with TSH.

2 SCOPE

This policy covers all passwords used for internal and external systems by users of any service in TSH and applies to all staff, volunteers and contractors or persons that have been provided with access to systems for a role within TSH. The term ‘system users’ will be used to cover all those listed.

This policy should be read in conjunction with any national policies, if available. Where there is a conflict of information, this policy overrides the national policies listed.

3 ROLES & RESPONSIBILITIES

3.1 Responsibilities of Users

All system users must abide by this policy.

3.2 Responsibilities of the State Hospital

TSH will provide controls to system passwords, where possible.

4 POLICY

4.1 Default Passwords

Any system that is purchased/acquired/obtained shall have any default/admin passwords changed immediately. Where the password cannot be changed the account should be disabled as soon as another account with the same privileges has been created.

4.2 Password Requirements

In any system that requires a password, system users will ensure, where possible, that a password chosen will protect access to that system to ensure the confidentiality and integrity of any identifiable or confidential information contained within that system. Passwords shall have the following mandatory characteristics:

- Password complexity: Where possible, system users will create complex passwords adhering to section 4.3. Where systems do not allow complexity, consideration should be given to creating passwords of extra length (i.e. three random 5-character words).

- Uniqueness: System users will create passwords that contain different characters i.e. not contain, in sequence, the same character or same number i.e. aaaaaa or 111111 or abcabcabc or aaa111.

- Difficult to guess: Passwords are created that are difficult to guess. This requires not using common passwords such as ‘Password1234’ or ‘Qwerty123456’. The password should not contain any or part of the usernames.

- Re-use of passwords: a new password shall not be the same as a password that was used previously. Some systems will enforce a password history which will prevent the use of the same password. This will vary from system to system.

- Contingency: If a password is recorded for any reason this should be recorded as securely as possible, i.e. not being recorded with a username or under a heading Password for {system name}. If a record is kept within a personal diary this should be locked away while not in use or if it is going to be left unattended for any length of time.

- Password checking: Some systems will check passwords, when created, for compliance with format and complexity.

- Account lockout: An account can be locked out after several failed attempts at entering a correct password. The system owner will provide the facility to unlock the account, and if necessary, provide a password reset option. The account holder may have to verify they are the account holder before unlocking the account and resetting the password.

- Password display: Where the option is available to display the password, system users should ensure this is done when the password cannot be viewed by someone else.

- Password changes: Different systems will request system users change their passwords at different intervals. System users should follow the guidance based on the system.

- Initial passwords: Passwords should be changed after an initial sign-in or change of password is requested:
  - System users should ensure the initial password that is provided to access a system is changed after the first sign-in. This should be completed with every system, even if the system does not require a change at first sign-in.
  - System owners should ensure, where possible, systems users are required to change the initial password after the first sign-in or after a password change is requested.

- Password sharing: Passwords should never be shared with other system users. On the occasion where password sharing is required i.e. access to a single account used by the organisation (purchasing, financial systems, technical support systems), system users should only disclose the passwords to those systems users that are authorised to access the same system. Where passwords have been disclosed for access to shared systems, these should not be disclosed further, without authorisation from the system owner or stored locally.

4.3 Password format

The minimum password complexity requirements are specified by the following rules, unless the system dictates otherwise:

- Shall not be the same as, or contain, the username.

- Shall contain characters, where possible, from three of the four categories:
  - Lowercase letters (a-z).
  - Uppercase letters (A-Z).
  - Numbers (0-9).
  - Special characters (Symbols) (! $ £ " @ %).

- Shall be at least 12 characters long. Where systems do not allow up to 12 characters, the maximum number of characters will be used.

4.4 Numeric Passwords

Where systems require a numeric password, sometimes referred to as a PIN (Personal Identification Number), these should follow the same guidance as Section 4.1 but with the following format:

- Shall be a minimum of six numbers.
- Will not be in sequence i.e. 123456 or 987654.
- Will not contain all the same number i.e. 111111 or 112233.
- Shall avoid being associated with the system user i.e. date of birth.

4.5 Password Integrity

System users should ensure their password is never shared with anyone. This can be achieved by following the steps below:

- Not tell anyone their password, this includes the system owner i.e. IT helpdesk staff, anyone claiming to be from IT or the system owner.
- Not allow anyone to watch when entering a password.
- Not allow the password to be printed out.
- Not disclose the password in any other way.
- Using a different password for different systems. This also includes using the same password for personal systems and systems used for work purposes.
- Change their password if they suspect it has been compromised and report the suspected compromise to the system owner at the earliest opportunity.

4.6 Password managers

TSH may deploy password managers to assist system users in recording the username and password for particular systems, to allow an automatic log in to that system. Only password managers authorised by the organisation should be used.

No personal password manager should be used to remember usernames or passwords used for TSH systems.

Password managers have the ability to record usernames and passwords for any system when a system user is logged into a computer. Care should be taken when accessing a system while someone else is logged into the computer as that could record someone else’s username and/or password for the system accessed.

Passwords should not be stored within web browsers. This option will be removed, where possible, but if the option is available, it should not be used.

4.7 Guidance on passwords

Guidance for creating passwords or passphrases is available on the Intranet under eHealth Department - Helpdesk FAQs and appended as Appendix 1: Password/Passphrase Guidance.

5 EQUALITY AND DIVERSITY

The State Hospitals Board (the Board) is committed to valuing and supporting equality and diversity, ensuring patients, carers, volunteers and staff are treated with dignity and respect. Policy development incorporates consideration of the needs of all Protected Characteristic groups in relation to inclusivity, accessibility, equity of impact and attention to practice which may unintentionally cause prejudice and/or discrimination.

The Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information/documents in alternative formats and are happy to discuss individual needs in this respect. If information is required in an alternative format, please contact the Person Centred Improvement Team on 01555 842072.

Line Managers are responsible for ensuring that staff can undertake their role, adhering to policies and procedures. Specialist advice is available to managers to ensure that reasonable adjustments are in place to enable staff to understand and comply with policies and procedures. The Equality and Impact Assessment (EQIA) considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

The volunteer recruitment and induction process supports volunteers to highlight any barriers to communication, physical disability or anything else which would prevent them from contributing meaningfully to patient care and / or engage in other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

6 STAKEHOLDER ENGAGEMENT

Consultation was undertaken at the time of policy development. Following review of the policy there have been no changes to current practice. Therefore engagement with Key Stakeholders has not been necessary for the 2025 review.

Key Stakeholders	Consulted (Y/N)
Patients	N/A
Staff	N/A
Carers	N/A
Volunteers	N/A

7 COMMUNICATION, IMPLEMENTATION, MONITORING AND REVIEW OF POLICY

This policy will be communicated to all stakeholders within The State Hospital via the intranet and through the staff bulletin. The Person Centred Improvement Service will facilitate communication with Volunteers.

The eHealth Sub-Group will be responsible for the implementation and monitoring of this policy.

Any deviation from policy should be notified directly to the policy Lead Author. The Lead Author will be responsible for notifying the Advisory Group of the occurrence.

This policy will be reviewed every three years, and when appropriate to consider changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner's Office.

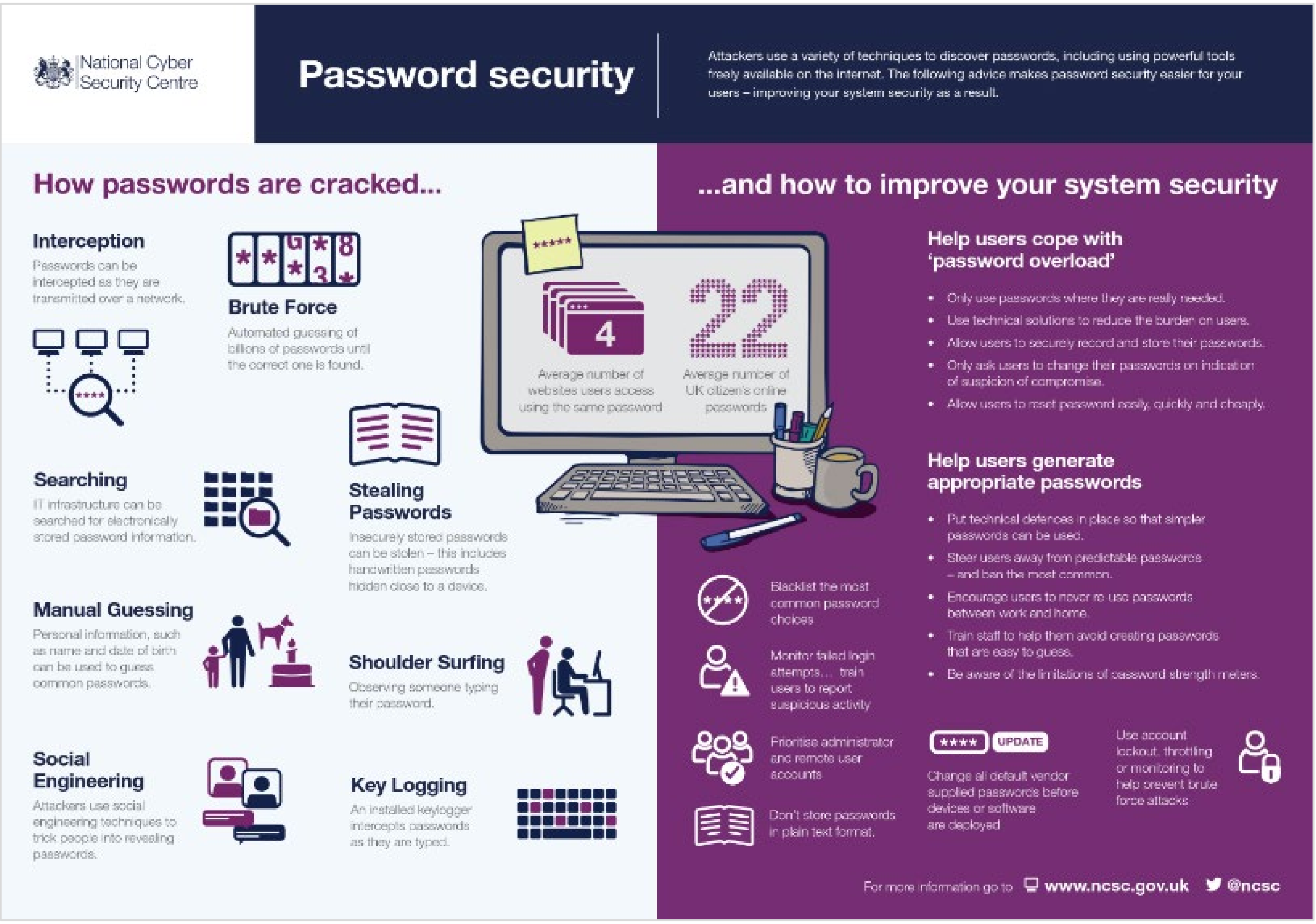
APPENDIX 1: PASSWORD/PASSPHRASE GUIDANCE

Password/Passphrase Guidance

The previous guidance of having an 8-character complex password has now changed (BBC article link below). The new guidance now advises that longer is better, when it comes to using passphrases or memorable information. The idea for this guidance is to help provide ways of creating complex passwords but still make them easy to remember.

Remembering passphrases is difficult, especially as there are many different systems that require passphrases. A recent report (BBC article link below) stated that people would usually require passphrases for an average of 22 different systems. If everyone had a unique passphrase for each of those systems that would be 22 passphrases that have to be remembered. This is why the majority of people will reuse the same password for many systems. This in itself is a security issue because if someone were to obtain one of your passphrases how many systems would they then have access to.

If you think of your own personal passphrases, outside of the workplace, which you use for your email, social media, online banking, utilities, shopping sites, etc, how many of those systems would be accessible if someone had access to one of the passphrases you use. Only your email? Your email and all your social media? Your email, social media and online bank?



National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception
Passwords can be intercepted as they are transmitted over a network.

Brute Force
Automated guessing of billions of passwords until the correct one is found.

Searching
IT infrastructure can be searched for electronically stored password information.

Stealing Passwords
Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing
Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing
Observing someone typing their password.

Social Engineering
Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging
An installed keylogger intercepts passwords as they are typed.

4
Average number of websites users access using the same password

22
Average number of UK citizen's online passwords

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc

If they know your passphrase, chances are they will know your email address which is usually your login details. Now think, if someone does have those details and can access your email and your online bank, what is stopping them changing your passphrase to stop you accessing those systems. Where is the link to change your password sent? Your email, and who now has access to that? How easy do you think it is to get your email password reset by whomever your email provider is?

For those of you who use NHS Mail as your main email account, what happens when you leave the NHS because you will not have access to it anymore? Having heard of different stories on the news and social media, it is not easy and can take weeks to get systems back to their rightful owner. Can you go that long without access to your mobile phone account, electricity account or online bank account?

When it comes to technology security start thinking, what disruption can this cause to me if that information gets into the wrong hands. Remember they do not even need to be in the same country as you to get that information.

Ideas for creating a long passphrase

Below are some methods that can help you create a new passphrase that meets the requirements. You do not have to use all the ideas and you can come up with your own versions but please remember you want to make it difficult to be guessed but easy to remember. Try to avoid names of family members, place of birth, something related to your favourite sports team or anything else that may be obtainable from social media.

A standard passphrase (expanding on the ones already released)

This method is basic and can be something you can associate with or due to its comedy value. There are not any restrictions with this method but remember to include capitals, numbers and special characters (!”£$%^&*()_ (a space is a special character as well)). Some examples of this method are:

- I love watching my daughter play rugby. High5.
- 10 chickens plus 2 cocks = more roast chicken dinners.
- What are my 5 passwords again?
- 1 Loves working here!

The only downside to using this method would be the need for different passphrases for each system, which again means the same phrase for many different systems will be re-used, which as highlighted above, can be a risk in itself.

System, random word, random item

This method allows the creation of a passphrase that can be unique for every system, based around a random word and a random item. For the examples below, I have chosen ‘hospital’ as the random word and a date of birth (DOB) of ‘2605’ for the random item. To take it a little further, for the date of birth (DOB), instead of just using the numbers, you can hold the shift key and then use the number to create the special character.

- hospital.Computer2605.
- Computer2605@hospital.
- emailhospital26)%.
- email@hospital2605.

With this method, you can reuse the random word and random item but change the system to reflect the system you are using. Taking the first example, you would change the system so that your computer login would be hospital.Computer2605 which for your email you would use hospital.Email2605 and for RiO you would use hospital.Rio2605. Even though all the passphrases seem similar, unless someone knows the random item(s) and the format you have chosen, it would be hard for anyone to guess or crack and allows. It also creates a unique passphrase for each system.

Think Random (NCSC)

Advice on the NCSC website (link below) states, “*We are working with Cyber Aware, advising that you create passwords using three random words. You just put them together, like 'coffeetrainfish' or ‘walltinshirt’.”*

This method can be a little difficult to remember, especially if you want to create multiple unique passwords. However, you can have a twist on this by introducing things that can be a little easier to remember, such as using someone’s DOB but reverse it 5062 or even part of someone’s phone number 2114. Then choose someone’s street name (not your own of course), LampitsRoad and then introduce something like your first car, Fiesta or first pet’s name, Spot. This would then make a password of 5062LampitsRoadFiesta or 2114LampitsRoadSpot. Remember to add in a special character somewhere to make the passphrase more difficult to guess.

Multi-Factor Authentication

Another form of securing accounts if the use of Multi-Factor Authentication. This is where using a passphrase is followed up by another method of verifying you are who you say you are.

This is a good method of stopping brute force attacks, where someone programs a system to try multiple passwords to access someone’s account.

Multi-Factor Authentication is becoming more widely used and can take a few forms. Multi means there will be multiple ways of confirming you are who you say you are but still have some draw backs. This is popular with mobile phones where you will get a text message when accessing something like an app or website. Even though this is multi-factor, if someone has access to your device that negates the second form of authentication.

This can be enhanced with another form of multi-factor which is classed as 2 Factor Authentication (2FA). This usually designed around the principle of have two out of three of the following:

- Something you are (fingerprint, retinal pattern, blood flow pattern).
- Something you have (mobile device, authentication token, Security pass).
- Something you know (password, passphrase, PIN, other memorable information).

Unlike the previous version of multi-factor authentication where you can authorise the access on the same device, 2FA requires as least two of the above i.e. a PIN number and a cashpoint/credit card or a randomly generated number sent via SMS and a fingerprint.

Useful links

News articles

- Password guru regrets past advice - https://www.bbc.co.uk/news/technology-40875534
- Internet users 'need 22 passwords' - https://www.bbc.co.uk/news/business-20726008

Password checkers

These can help you check the how secure your current password is and if you are planning to change it, how secure your new passphrase will be. We would advise not using your exact password/passphrase on these sites but use something of the same length and complexity. Even if you find your password/passphrase appears to be secure try adding one more character to see how more secure that will be, relating to the time it will take to crack.

- https://www.security.org/how-secure-is-my-password/
- https://www.my1login.com/resources/password-strength-test/

Account checker

The following sites can be used to check if you email address or phone number has been obtained during a third party compromise. This is where you have given your details to a legitimate website/business, who in turn have been hacked/compromised and your details obtained. Running a check on the following site will show if your email address or phone number have been obtained and posted online for people to obtain or purchase. The results will also show the extent of the information obtained.

https://haveibeenpwned.com/

Password generators

These sites can be handy for generating random passwords but may be too complex for everyday use. You can use these passwords for systems that either do not require the entry of the password regular, such as your wireless password or for a one-off password.

- https://passwords-generator.org/
- https://my.norton.com/extspa/idsafe?path=pwd-gen
- https://www.passwordcard.org/en

NCSC (National Cyber Security Centre)

- https://www.ncsc.gov.uk – NCSC Main site.
- https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0 - Three random words or #thinkrandom article.
- https://www.cyberaware.gov.uk/ - Cyber Aware Main site.