Policy:

IMST 001 Password

Executive Director lead	Executive Director of Finance
Policy Owner	Assistant Deputy Director of Operations & Services
Policy Author	IT ServiceDesk Manager

Document type	Policy
Document version number	3.0
Date of approval	28 June 2021
Approved by	ARC/FPC
Date of issue	July 2021
Date for review	June 2022

Summary of policy

This policy is to establish, govern and promote security best practices for account password management across all Information and Communication Technologies (ICT) related systems throughout the Trust.

Target audience	All Trust employees & the Trust Board

Keywords	Password Policy

Storage

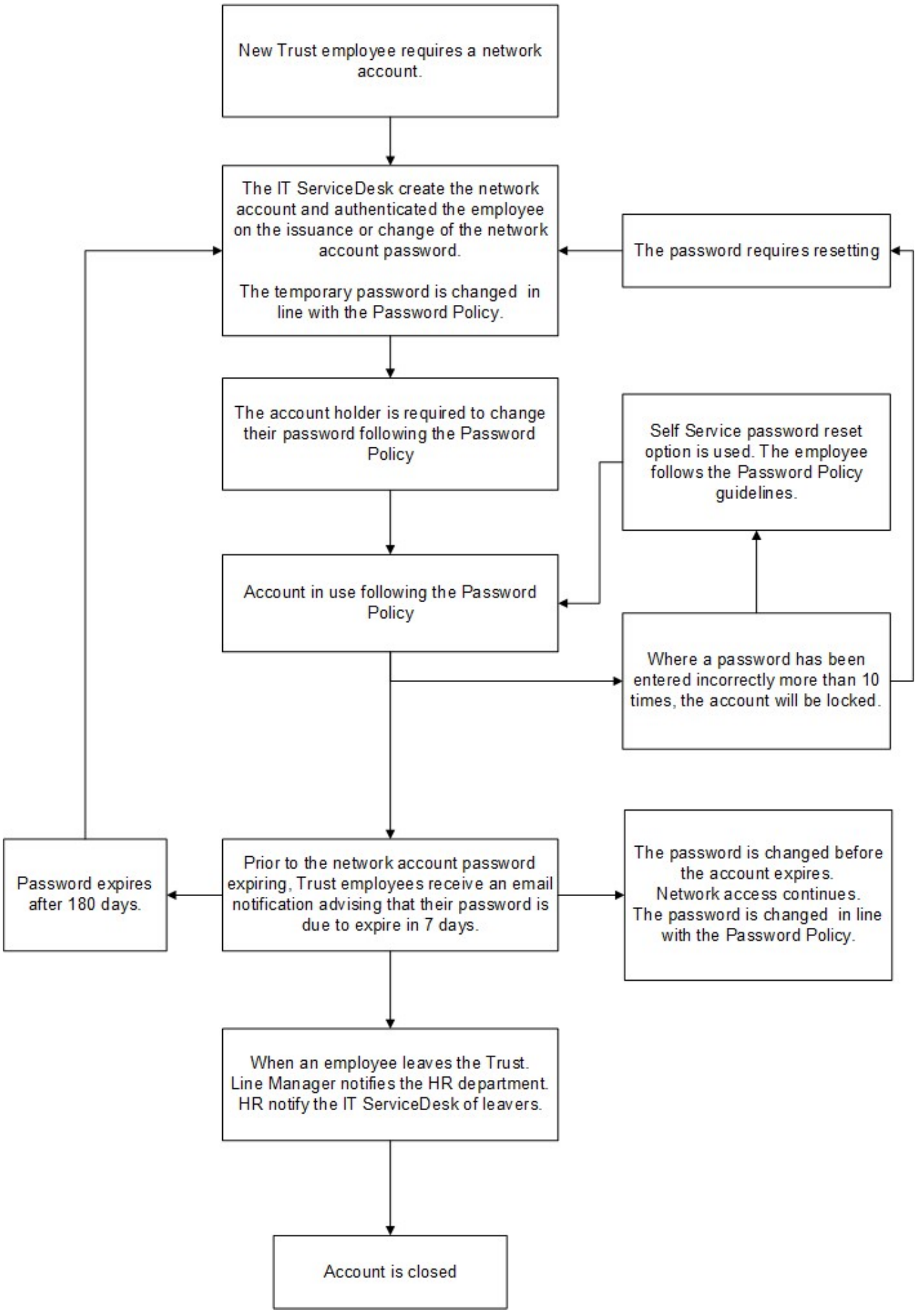
Version 3.0 of this policy is stored and available through the SHSC intranet/internet. This version of the policy supersedes the previous version 2.0 June 2020. Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
0.1	New draft policy created	11/2016	New policy commissioned by IMST part of the Cyber Strategy to secure and protect IT Infrastructure.
1.0	Approval and issue	09/2017	Amendments made during consultation, prior to ratification.
2.0	Review / approve / issue	06/2020	Recommendations from Annual Penetration Test March 2020 on Trust Infrastructure.
3.0	Review / approve / issue	06/2021	Amendments made based on the results of the Dionach IT Health Check Assessment. Results highlighted the requirement to strengthen the Trust password security. Amendments to Section 7 & 7.6

Contents

Flowchart


New Trust employee requires a network account.
The IT ServiceDesk create the network account and authenticated the employee on the issuance or change of the network account password.
The temporary password is changed in line with the Password Policy.
The password requires resetting
The account holder is required to change their password following the Password Policy
Self Service password reset option is used. The employee follows the Password Policy guidelines.
Account in use following the Password Policy
Where a password has been entered incorrectly more than 10 times, the account will be locked.
Password expires after 180 days.
Prior to the network account password expiring, Trust employees receive an email notification advising that their password is due to expire in 7 days.
The password is changed before the account expires.
Network access continues.
The password is changed in line with the Password Policy.
When an employee leaves the Trust.
Line Manager notifies the HR department.
HR notify the IT ServiceDesk of leavers.
Account is closed

1 Introduction

This policy describes the Password Policy for Sheffield Health and Social Care NHS Foundation Trust (SHSC) referred to in this document as the Trust.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Trust's entire corporate network. As such, all Trust employees, including Non-Executive Directors, Governors, partner agencies, contractors, volunteers and vendors with access to Trust systems will be referred to as 'employees' throughout this document. All employees are responsible for taking the appropriate steps, as outlined in this policy, to select, use and secure their passwords.

This policy is written in compliance with legal and contractual obligations including:

- General Data Protection Regulation/Data Protection Act (2018) - require that personal data be kept secure against unauthorised access or disclosure. The password is part of the security environment.

- The Computer Misuse Act (1990) - covers unauthorised access to computer systems, including the use of another person's identity. If a user "lends" their account and password to another individual who then breaches the Computer Misuse Act, both the individuals concerned would be deemed to have committed an offence.

2 Scope

This policy applies to all Trust IT systems and employees, who:

- Have or are responsible for any network account or resources (or any form of access that supports or requires a password) on any system that resides at any of the Trusts facilities
- Have access to the Trust's data network using any device
- Store any non-public Trust information.

New accounts and passwords are created on completion of the new starter process. Please refer to the new starter process for further details.

3 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change across all Information and Communication Technologies (ICT) related systems throughout the Trust.

4 Definitions

For the purpose of this policy all systems provided by the Trust requiring a password are covered by this policy. This policy relates to the Trust domain to which employees log onto.

5 Detail of the policy

The broad overview of this policy is as described in the introduction.

6 Duties

All staff

Implementation and adherence to this policy is the responsibility of all Trust employees. 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.

All employees have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Trusts Incident Management Policy (Incident reporting form that can be accessed on any Trust PC/laptop using the E-Incident login icon on the desktop). Breaches will then fall under the Incident Management reporting policy that can be found on the Trust intranet pages. (https://nww.xct.nhs.uk/index/widget.php?wdg=wdg_policies)

This obligation also extends to any external organisation contracted to support or access the Information Systems of the Trust.

The Board

The Board is responsible for:

- Ensuring robust incident reporting, investigation and management systems are in place and that these are monitored and reviewed and compliant with external regulation
- That serious incidents are reviewed, and recommendations/actions implemented

Executive Directors

Executive Directors are responsible for:

- Commitment through endorsement of this policy
- Final approval of the policy
- Performance management of incident management procedures.

Data and Information Governance Group (DIGG)

The Data and Information Governance Group is responsible for:

- Approving the policy for review by the Digital Transformation Board/Executive Directors.

Managers

Department Managers/Line Managers are responsible for:

- Ensuring staff are aware and comply with this policy**,** ensuring that staff have access to the policy and any relevant training.
- Notifying the IMST Department of any leavers or personnel changes that require a change to accounts or passwords.
- Following Trust Policy, investigating breaches of policy by leading a reasonable, thorough and fair review of the investigation with support from Human Resources as appropriate**.**
- Completing a written report of review/outcomes and providing appropriate written feedback to all parties, with advice from Human Resources.
- Ensuring confidentiality during investigations, briefing participants on their responsibilities or confidentiality and taking or referring for appropriate

action should confidentiality be breached.

Human Resources

Human Resources is responsible for:

- Advising staff and managers on the policy and associated procedures monitoring the policy, as appropriate ensuring the policy is adhered to throughout.
- Supporting Line Managers and investigating manager as appropriate.

Contractors and Vendors

In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Trust systems or network, results from the non-compliance, the Trust will consider legal action against the third party.

The Trust will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place.

7 Procedure

The Trust's main network enables user logons and authentication via a unique username and password. Unique authentication is the security boundary for the majority of systems in use and accessed by Trust employees, both internal and external to the Trust.

With continuing reliance on ICT systems, it has become increasingly important to ensure the integrity of all system/access logon accounts used across the Trust is maintained. The following procedures and practices must be followed to ensure the security and integrity of these accounts.

All systems used by the Trust (supported by IT or other departments) should where technically able, adhere to the following password guidance. Where systems do not have the capability of adhering to the policy guidelines, the details should be entered onto the risk register. All future systems procured by the trust should adhere to this policy. Details of the current core system password requirements are provided in appendix B.

Please refer to the policy exclusions for further guidance in section 7.8.

Requirements for all Trust staff:

- All users must ensure that their passwords are not divulged or shared with anyone else.
- All users **must** create passwords that fall into the category of strong passwords under the construction guidelines within this policy (section 7.3)
- All users must not write down and/or store passwords on paper
- All users must not store passwords on unencrypted electronic devices (e.g. applications on smartphones, USB storage devices etc)
- Passwords must not be inserted into email messages or other forms of electronic communication
- All users should use different passwords for different systems/applications
- Use passwords that are not used for personal accounts
- Do not re-use previous passwords
- Temporary passwords must be changed as soon as possible
- If an account or password is suspected to have been compromised, the incident must be reported to the IMST ServiceDesk Team and via the

procedures set out in the Incident Management Policy. Immediately change any/all passwords which may have been compromised.

Additional requirements for IMST staff and ICT systems/services:

- Ensure future systems enable and meet the minimum password length and complexity requirements as set out under the high-level password guidelines within this policy.
- Where technically able, systems should support banned password list technologies to prevent the use of common or bad passwords.
- Change all default passwords before the deployment of ICT systems/services.
- Where secure and technically able, systems should support single sign on (SSO) authentication.
- Where technically able Internet facing services should support Two factor Authentication(2FA) or Multi Factor Authentication (MFA)
- Carry out regular audits/checks of system devices and software to highlight default passwords and change these to strong passwords in line with this policy.
- All ICT devices which may require local logon privileges for configuration and maintenance i.e. Printers, network switches, routers, SAN (storage area network) appliances etc… must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of this policy wherever possible.
- Support individual user authentication – providing for identification of specific users and not groups
- Where technically able, prevent the storing of passwords in clear text or in any easily reversible form
- Support password expiry functionality where accounts are set to expire after 180 days
- Provide for the management of specific roles and functions within a system enabling the delegation of tasks to individuals
- Where technically able, not contain or utilise embedded (hard-coded) or default passwords – these are passwords which are “fixed” (saved) on a computer or device and are often “hidden” from view. Embedded passwords can be used as a “back door” to computers and systems and must be prevented
- Use access control procedures, which apply to both operational and test systems equally
- All externally procured software must satisfy the requirements of this policy and enable passwords that meet the high-level account password guidelines in section 7.1.1
- Password cracking or guessing will be performed on a periodic or random basis during audit penetration tests involving 3rd party companies. All audit penetration tests must be approved by the Director of Finance (Audit) and the Data and Information Governance Board prior to the work commencing.
- Prioritise essential infrastructure devices.

7.1 Password Guidelines

Passwords are used for various purposes at the Trust. Examples of some of the more common password used include: user level accounts, web accounts, email accounts, local access to ICT devices such as routers, printers etc. Details of the current core system requirements are outlined in appendix D.

Password complexity is outlined as 2 levels, high and entry level, as detailed below.

7.1.1 Guidelines for high-level account passwords.

High-level accounts provide increased network access to fulfil administrative functions. Typically, high-level access is provided to IMST staff, for use in providing PC and network administrative support. High level account passwords must contain:

- A minimum password length of 20 characters
- Must not contain any part of the username
- Passwords must meet complexity requirements – this forces the use of passwords which must contain at least three of the four following elements:

    1. Numeric – (0-9)
    2. Uppercase – (A-Z)
    3. Lowercase – (a-z)
    4. Special Characters (?,!, @, #, %, etc…)

High level accounts are set to expire at 360 days and lock out after 10 minutes of inactivity.

7.1.2 Guidelines for entry level account passwords.

On joining the Trust all employees are provided with an individual (Active Directory) network account logon. The entry level account provides access to the Trust's network and associated systems and should be a minimum of 12 characters long. Details of the current system requirements are outlined in appendix G.

Entry level accounts are set to expire at 180 days and lock out after 10 minutes of inactivity.

7.2 Generic Passwords

The use of generic passwords is not permitted. In exceptional circumstances where this is unavoidable their use requires consent by the Data and Information Governance Board. Accountability of generic accounts requires monitoring via other means.

7.3 Strong Password Guidance

All staff should be aware of how to construct and select strong passwords. The more letters, special characters and numbers used and the longer the password is, the stronger the password will be.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits, punctuation and special characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least twelve alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, such as names of family or dates of birth, username, etc.
- Are not used for authentication to other systems/applications where single sign on authentication is not enabled.
- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered.
- Passwords should not be based on the previous passwords.

Strong passwords can be created by:

- Passphrases –Typically passwords will consist of letters, numbers and special characters which are used to represent the words or meaning of a phrase. E.g. ‘I catch the number 14 bus on Fridays’ could become iCatchthe number14bu$.
- Using a random mix of numbers, symbols and different case letters e.g. rainbow could become ra!nB0w$.
- Using the keyboard – using letters one row above so that ‘password’ could become ‘0qwW294e

IMPORTANT: The above passphrase/password is an example and must NOT be used

7.4 Password Protection Standards

- Do not use the same password you use for Trust account/s for other non-Trust access (e.g., personal internet service provider (ISP) account, personal banking, online shopping etc.).
- Where systems are secure and technically able, single sign on (SSO) authentication will be used for access to Trust systems. SSO enabled applications utilise windows authenticated logons for a number of separate IT systems.
- Do not share Trust passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Trust information.

Good practice rules:

- Don’t reveal a password to ANYONE or share passwords with colleagues
- Don't reveal a password over the phone to ANYONE - unless relaying information on temporary passwords which are changed immediately
- Don’t write passwords down and store them anywhere (e.g. in the office, home or elsewhere)
- Don't reveal a password in an email message - unless relaying information on temporary passwords which are changed immediately
- Don't reveal a password to your line manager
- Don’t use passwords that contain all or part of the account name
- Don’t use passwords relating to common words (e.g. year, month)
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on holiday
- Don’t write down, store or communicate any security answers used to reset passwords that have been forgotten or require changing
- Don’t leave your account open and/or unattended, leaving accounts/passwords vulnerable to abuse
- If someone demands a password, refer them to this document and request that they call the IMST Customer Services Team
- Don’t use the "remember password" feature of applications (e.g., Internet Explorer, SAP etc…).
- Don’t store passwords in a file on ANY computer system (including mobile devices or similar) without encryption. (IMST operate approved password management software for privileged accounts).
- Do lock your computer when leaving it unattended.

7.5 Password Expiry

All Trust accounts should be set to expire within 180 days depending on the account type. Accounts not used within 6 months will be disabled/deleted. Where an account requires re-enabling contact the IMST Customer Service Team (IT.ServiceDesk@shsc.nhs.uk)

Passwords are set to expire at 180 days to:

1. To improve network security

2. To improve the complexity requirements for the setting of passwords

Windows software Users (i.e. PC/laptops and not tablet users) are prompted to change their password at logon **7** days prior to the existing one expiring. All Trust staff will receive an email notification to advise them that their password will expire in 5 days. Where passwords are not changed following the email notification, further emails will be received until the password is changed.

Nationally managed systems using Smartcards currently expire after 2 years and are exempt from the 180 days password expiry set for all other Trust used system. Please refer to section 7.7 for further details.

7.6 Password Lockout and Reset

Trust computer screens are set to lock after 10 minutes of inactivity. After this time Users will be required to re-enter their password to open the computer for use.

Where a password has been entered incorrectly 10 times the account will be locked and can only unlocked by contacting IT ServiceDesk or Self Service Reset Password Management Tool (SSRPM) from a Trust desktop or laptop connected to the corporate network.

Where possible passwords can be reset using SSRPM or by contacting the IT ServiceDesk Team (IT.ServiceDesk@shsc.nhs.uk) who will verify account holder's answers against three security questions in the SSRPM system.

Reset passwords are unable to be set to any of the previous 24 passwords.

Once a password has been changed it can be reset using the Microsoft Windows change password option. The Windows change password option is accessible by pressing the keyboard control (ctrl), alt and delete buttons simultaneously.

Equipment installed with the Bitlocker program will have a Trusted Platform Module (a chip in the hardware designed to disable the hardware after several failed logon attempts) enabled.

The TPM module locks out those machines, where the encryption password has been entered incorrectly on 32 consecutive occasions. Equipment locked out using this method cannot be unlocked and staff should contact IT ServiceDesk.

7.7 Mobile Phones

Trust mobile phones must be protected with a minimum 4-digit personal identification number (PIN). Where capable, Trust mobiles should also be protected through the use of fingerprint identification.

On approval of the personal mobile device form, Trust employees using personal devices, are subject to the same password conditions as Trust mobiles.
Personal and Trust mobile phones, accessing Trust information/systems (e.g. email, calendars etc), agree to terms and conditions allowing the use of remote data removal where applicable i.e. lost/stolen phones.

Where PIN identification is entered on the device incorrectly more than 6 times, the device will automatically be wiped. Please refer to the Data & Information Sharing Policy for further guidance including information on sending confidential information.

Please refer to the Remote Working and Mobile Devices Policy for further guidance.

7.8 National Systems - Smartcards

National systems (such as the Electronic Staff Record (ESR) system) access is granted through the use of role-based access using Smartcards. Systems using Smartcard functionality use certificates which expire after 2 years. After this time all access is removed unless access/certificates are renewed by an appropriate Sponsor.

Role-based access is granted through Sponsor approval and therefore Sponsors must notify the Smartcard Management service (Registration Authority) of leavers and access removal in a timely manner.

8 Development, consultation and approval

- 2016\17 policy created and developed in 2017 by IT ServiceDesk Manager following national guidelines.
- Nov 2017 policy agreed and published
- April 2020 policy reviewed and amended in accordance with the IT Infrastructure Annual Penetration Test (conducted by ChessSecurity 03/2020) and the IT Internal audit recommendations.
- May 2020 password recommendations presented and agreed at the Data Information Governance Group (DIGG) meeting. Documented in DIGG meeting notes.
- Review and seeking approval of policy amendments by Policy Governance Group of June 2020.
- June 2021 policy reviewed and amended in accordance with Dionach Cyber Assessment
- Review and seeking approval of policy amendments by Policy Governance Group of June 2021.

9 Audit, monitoring and review

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Policy in regard to IT Security – Password management	Review of IT ServiceDesk incidents and service requests	IT ServiceDesk Manager	Annual	IT ServiceDesk Manager	Data Information Governance Board	IT Operations and Services Teams
IT Infrastructure and data protection and integrity	In line with Cyber Security best practices and guidance or recommendation from annual IT penetration test	IT Operations Team Lead	Annual	IT Operations Team Lead	Data Information Governance Board	IT Operations and Services Teams
Information Data Security	NHS Data Security & Protection Toolkit guidance and compliance	Data Protection Officer	Annual	Data Protection Officer	Data Information Governance Board	Data Protection Officer

The policy will be reviewed periodically to ensure compliance with legal requirements and as a minimum every three years. Review of this policy is the responsibility of the IMST department.

10 Implementation plan

On approval of the Data and Information Governance Board, the policy will be made available on the policies section of the Trusts intranet. All staff will be advised of the policy via communications publications. New starters will be made aware of the relevant policies by departmental Managers.

Where applicable systems Managers will be required to update all IT system to adhere to this policy.

Action / Task	Responsible Person	Deadline	Progress update
Upload revised policy onto intranet and remove old version	*IT Operations Team Lead*	30/07/2021	*Following policy approval*
Make teams aware of new policy	*Team managers*	*30/07/2021*	Internal team communication
Communications awareness	*Communication Team*	30/07/2021	*Following policy approval*

11 Dissemination, storage and archiving (Control)

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.0	01/10/2017	01/10/2017	n/a	
2.0	21/06/2020	21/06/2020	22/06/2020	
3.0	July 2021	July 2021	July 2021	
4.0				

- This is version 3.0 and is available through the SHSC intranet/Internet policy repository and supersedes the previous version 2.0 (June 2021).
- Any copies of the previous policy held separately should be destroyed and replaced with this version.
- All versions of IMST policies are stored on the IMST shared directory and are available on request.
- Word copies of final versions of policies can be obtained from Policy Governance via the PA to the Director of Human Resources.

12 Training and other resource implications

Department Managers are responsible for ensuring that their staff are aware of and comply with this policy.

13 Links to other policies, standards (associated documents)

This policy forms part of the Trusts information governance policies and should be read in conjunction with the Trust IT and information governance policies that can be found on the intranet https://jarvis.shsc.nhs.uk/documents?keys=&category=All&document_type=205

Please refer to the Email Policy and Mobile Communication Devices Policy for guidance relating to the sending of confidential information and mobile devices.

14 Contact details

Title	***Name***	***Phone***	***Email***
IT ServiceDesk Manager	Keeley Parker	0114 3050738	Keeley.Parker@shsc.nhs.uk
IT Operations Team Lead	Emma Porter	0114 2718177	Emma.Porter@shsc.nhs.uk
Data Protection Officer	John Wolstenholme	0114 3050749	John.Wolstenholme@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement. **I confirm that this policy does not impact on staff, patients or the public.**	***I confirm that this policy does not impact on staff, patients or the public.*** Name/Date: Emma Porter	**YES,** Go to **Stage 2**

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age	**No**	**No**	**No**
Disability	**No**	**No**	**No**
Gender Reassignment	**No**	**No**	**No**
Pregnancy and Maternity	**No**	**No**	**No**

Race	**No**	**No**	**No**
Religion or Belief	**No**	**No**	**No**
Sex	**No**	**No**	**No**
Sexual Orientation	**No**	**No**	**No**
Marriage or Civil Partnership	**No**		

Please delete as appropriate: - no changes made.

Impact Assessment Completed by:
Name /Date Emma Porter / 02/06/2020

Appendix B – Core System Password Requirements

Core System/ Description	Authentication	Current Password requirements

Windows Authentication Active Directory Standard Network Account	Individual username and password	Password requirements:
		• minimum of 12 characters
		• passwords must meet complexity requirements – this forces the use of passwords which must contain at least three of the four following elements:
		  ○ Numeric – (0-9)
		  ○ Uppercase – (A-Z)
		  ○ Lowercase – (a-z)
		  ○ Special Characters (?,!, @, #, %, etc…)
		• Introduction of banned password lists
		• Password Expiry: 180 days

Administrative Windows Authentication
 	
Administrative Trust server/network/PC access
	Individual username and password	Password requirements:
		• minimum of 20 characters
		• passwords must meet complexity requirements – this forces the use of passwords which must contain at least three of the four following elements:
		  ○ Numeric – (0-9)
		  ○ Uppercase – (A-Z)
		  ○ Lowercase – (a-z)
		  ○ Special Characters (?,!, @, #, %, etc…)
		• Introduction of ban password lists
		• Password Expiry: 360 days

Insight *Clinical System*	Individual username and password	Password requirements: • between 6-15 characters • cannot contain the same repeated character • must not contain any of the following special characters: = [ ] ' , % " " ! @ $ • not contain the following words: Password, Insights, Monday.....etc • not contain part of your name. Password Expiry: 40 days.
JAC *Prescription System*	Individual username and password	Password requirements: • minimum of 8 characters • must include a minimum of 1 uppercase letter, 1 lowercase letter and a numeric character. Password Expiry: 180 days.

E-Learning *Electronic training system* *(NB – links to the ESR system)*	Individual username and password ESR colleagues - Smartcard synchronisation then individual username and password	Password requirements: • minimum of 8 characters • must include a minimum of a letter and a numeric character • must not contain repeating characters • must not contain words listed under the E-learning restricted words (contact the E-learning Team for more detail). Password Expiry: 60-90 days.
EMAR System *Medicines Management system*	Individual username and password	• No minimum password requirements Password Expiry: 100 days.
E-Rostering *Electronic work force management system*	Individual username and password	Password requirements: 1. Initial password and remote access: • minimum of 6 characters • can contain alphanumeric character • must not contain symbols or spaces • password suspended after 5 incorrect attempts to be reset by the E-rostering Team.
Electronic Staff Record (ESR) *HR staff record system*	Smartcard role-based access	Smartcard password requirements: • A choice of between a minimum of four to eight alpha and / or numeric characters Password expiry on notification or 2-year expiry of 'certificate' access.
Integra *Finance System*	Individual username and password	Password requirements: • minimum of 6 characters • passwords must contain at least 1 mandatory digit. Password Expiry: 90 days.
NHSmail *Email System*	Individual username and password	Password requirements: • must not be based on the username • must contain characters from 3 of the following 4 categories: 1. uppercase letters (A-Z) 2. lowercase letters (a-z) 3. numbers (0-9) 4. non-alphanumeric characters (e.g. ! $ # %) 5. must be at least 8 characters long 6. must not repeat any of the last 4 passwords 7. must not contain spaces or commas.

		Password Expiry: 90 days.
Tablet & Smartphone Email/Insight system access	PIN number	Password requirements: • 4-digit PIN • Not contain the same numbers. No password expiry.

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Yes/No	Evidence
	Executive Lead – Finance Director		
1.	Is the Executive Lead sighted on the development or review of the policy?	Yes	Recommendation for policy change discussed and approved by DIGG
2.	Is the team/Directorate PGG member sighted on the development of the review of the policy?	Yes	
	Development and Management of Policies		
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process, *insert hyperlink to Case for Need process*?	N/A	
4.	State the reasons for development of the document	Yes	Audit 360 Dionach Assessment Outcomes
5.	Please confirm the individuals involved in the development of the policy?	Yes	Keeley Parker John Wolstenholme Emma Porter
6.	Is the policy title clear and unambiguous and meets the requirements of the Policy on Policies, *insert hyperlink to policy,*	Yes	
7.	Does the style and format of the policy meet with the requirements of the Development, Management and Review of Policies?	Yes	
8.	Has it been completed in line with the template?	Yes	
9.	Is the policy in Arial font 12?	Yes	
10.	Have page numbers been inserted? Please make sure that there is no page number showing on the front cover, version control or contents pages	Yes	
11.	Does the policy contain a list of definitions of terms used?	Yes	

12.	Has the policy been quality checked for typographical errors, links, accuracy etc.	Yes	
13.	Does the policy include any references to other associated policies and key documents	Yes	
14.	Is there evidence of consultation with all relevant teams and directorates e.g. HR, Finance, Procurement?	Yes	
15.	Has the policy been discussed and agreed by the local governance groups e.g. Medicines Optimisation Committee, or Trustwide specialist groups e.g. Resuscitation and Physical Health Group	Yes	Recommendation raised and agreed in DIGG 19/04/2021.
	Policy Content		
16.	Is the document linked to a strategy?	Yes	Cyber Security strategy
17.	Is the purpose of the policy clear?	Yes	
18.	Are the intended outcomes of the policy described?	Yes	
19.	Does the policy reference requirements of the CQC or other relevant bodies e.g. NHSLA RMSAT, if applicable?	N/A	
20.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.	Yes	Respond to outcomes recorded in the annual security penetration test in compliance with DSPT
21.	Are supporting references cited in full?	Yes	
22.	Are Trust supporting documents referenced?	Yes	Password Practices 21/06/2021 DIGG Paper
23.	Has the EIA Form been completed (Appendix A)?	Yes	
	Policy Verification and Ratification		
24.	Have Staff Side (or equivalent) approved the document (HR policies only)? All policy documents must be initially verified through the appropriate governance group to ensure that they are accurate, valid and fit for purpose. Advice on which governance group to approach is available from the Director of Corporate Governance.		

These groups include:

Type of Policy	Governance Group
Corporate	Quality Assurance Committee (QAC) Audit Risk Committee (ARC)
Health and Safety	Service User Safety Group Health and Safety Committee
Human Resources	Joint Consultative Forum Policy Group (JCF)
IT	DIGG
Local Guidance, etc	Local Governance Group
Medicines	Medicine Management Committee
Mental Health	Mental Health Act Group
Risk Management	Service User Safety Group Health and Safety Committee
Safeguarding	Safeguarding Children and Adult Steering Group

	Dissemination and Implementation		
25.	Does the dissemination plan identify how dissemination will be implemented, see 11 of Policy on Policies	Yes	
26.	Does the dissemination plan include the necessary training/support to ensure compliance?	N/A	Should be included as staff mandatory training and starter induction.
	Document Control		
27.	Have you included version control on the document?	Yes	
28.	Does the document identify where it will be held? See Storage on policy cover sheet.	Yes	
	Process for Monitoring Compliance		
29.	Is there a plan to: i. Review ii. Audit compliance with the document	Yes	
	Review Date		
30.	Is the review date identified?	Yes	June 2021
	Overall Responsibility for the Document		
31.	Who will be responsible for co-ordinating the:		IT Operations Team Lead IT ServiceDesk Manager

	i. Dissemination ii. Implementation iii. Evidencing iv. Monitoring		