NHS
Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

IT Password Policy

Shaping better health

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	50
Responsible Executive Director:	Sarah Truelove, Deputy CEO and Chief Finance Officer
Author and Job Title:	Jane Schofield, Digital Business Partner
Date Approved:	March 2020
Approved by:	Sarah Truelove, Deputy CEO and Chief Finance Officer
Date of next review:	March 2022

	Yes/No/NA	**Supporting information**
Has an Equality Impact Assessment Screening been completed?	Yes	
Has the review taken account of latest Guidance/Legislation?	N/A	
Has legal advice been sought?	N/A	
Has HR been consulted?	N/A	
Have training issues been addressed?	Yes	
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by JCC?	N/A	
Are there financial issues and have they been addressed?	No	None identified
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	Yes	This is one of several policies produced by SCW CSU comprising the Information Security Management System
Has the lead Executive Director approved the policy?	Yes	
Which Committees have assured the policy?	N/A	The document has been reviewed by the Corporate Policy Review Group
Has an implementation plan been provided?	Yes	
How will the policy be shared with: • Staff? • Patients? • Public?		See Implementation Plan
Will an audit trail demonstrating receipt of policy by staff be	No	

required; how will this be done?		

Contents

Password Policy

1. Introduction

This document forms part of the Information Security Management System that is maintained by NHS South, Central and West Commissioning Support Unit (SCW) on behalf of Bristol, North Somerset and South Gloucestershire Clinical Commissioning Group (BNSSG CCG).

This document provides detailed policies that govern the usage of passwords.

1.1. The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that:-

- Set out the governance of IT security.
- Provide high level policy statements on the requirements for managing IT security.
- Define the roles and responsibilities for implementing the IT security policy.
- Identify key standards, processes and procedures to support the policy.
- Define security architectures that encapsulate the policy and support the delivery of secure IT services.

There are several policies which comprise the ISMS which include the following:

Acceptable Use of It Policy

Clear Screen Policy

Network Security Policy

IT Disposal Policy

Anti-Virus Policy

Information Security Policy

Some of these policies which have been agreed by BNSSG govern the operation of the IT estate provided by SCW CSU.

1.2. Document Purpose

This document provides the detailed password policy statements that support the overall IT security objectives of BNSSG CCG as set out in the security statement in the ISMS.

2. Details of the Password Policy

2.1. Policy Overview

The policy describes how users of BNSSG CCG supported systems should create and manage their passwords. This policy applies to all systems, including those which currently do not have an enforced password change process.

2.2. Policy Audience

This policy applies to all BNSSG CCG employees including temporary staff, sub-contractors, contractors, third parties and customers with access to BNSSG CCG information, information systems and services. In this document the audience described here will be referred to as users.

2.3. Policy Detail

- Users must not disclose their password by any means.
- Users must choose a password that is not easily guessed by others, for example the following are **not** suitable – dictionary words, car makes, telephone & room numbers; forenames and surnames; common words e.g. colours, seasons, days, sports, beverages etc.; simple keyboard sequences e.g. qwerty; words associated with computers.
- BNSSG CCG logon passwords must be changed every two months (automatically enforced). Where enforced changes are not present, the user should manually change the application password. Users will be at times directed by the password parameters of individual systems
- Passwords must normally have a minimum of 8 characters.
- It is acknowledged that most tablets and smartphones issued by BNSSG CCG are currently protected by four-character passwords pending a solution for these devices to comply with this policy.
- Users must ensure their BNSSG CCG password is different from any other passwords they use to access non-BNSSG CCG systems or devices.
- Users must ensure that password consists of a mix of at least 3 of the following types of characters:
  alpha (uppercase),
  alpha (lowercase),
  numeric characters and
  special characters (i.e. punctuation).
- System level passwords (e.g. Root, Administrator, Service Accounts) must be stored within an encrypted password vault.
- Privileged users should be provided with an alternative account with a password different to their standard login.
- Where a user has reason to believe that their password has been disclosed to others, they must change it immediately and must report this as a potential security incident with

the IT Service Desk who will determine if any immediate action is required. The user should also report any information governance / security related incidents to their departmental information asset owner, who will make a decision as to whether the incident should be reported onto Datix. If logged on Datix, the CSU information governance (IG) team will investigate the incident

- All users are responsible for reporting any suspected misuse of passwords.

Passwords on personal mobile phones

BNSSG supports the use by staff of their own personal mobiles so long as this does not compromise an individual's safety. Where an individual chooses to use a personal device, work related data cannot be stored on this device. In the event that a personal device is used, the individual must set a password to secure the device and this password must be a minimum of 6 characters. Access to work related information available on any personal device must not be allowed and the individual is responsible for restricting access.

3. Public Sector Equality Duty – Equality Impact Assessment

The Equality Act 2010 requires public bodies to consider the needs of all individuals in their day to day work. At BNSSG CCG we do this by completing an Equality Impact Assessment as described in the Equality and Diversity Policy which can be found, along with the assessment form, on the ConsultHR intranet site. If you need help identifying potential equality issues you should contact BNSSG CCG equality and diversity lead.

4. Policy Non-Compliance

Any breach of this policy could result in disciplinary action and possible ICO action if information loss occurs.

5. Review of Policy

As part of the Information Security Management System this policy will be reviewed on an ongoing basis by the BNSSG CCG senior management team.

6. Counter Fraud

The CCG is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document.

7. Appendices

7.1. Equality Impact Assessment

1. Title of policy/ programme/ framework being analysed IT Password Policy.
2. Please state the aims and objectives of this work and the intended equality outcomes. How is this proposal linked to the organisation's business plan and strategic equality objectives? To provide a framework of guidance to Bristol, North Somerset and South Gloucestershire Clinical Commissioning Group (BNSSG CCG) staff (as defined in the scope) regarding the security of Personal and Sensitive Data in both paper and electronic form.
3. Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers Staff.
4. What evidence do you have of the potential impact (positive and negative)? None expected.
4.1 Disability (Consider attitudinal, physical and social barriers) No impact
4.2 Sex (Impact on men and women, potential link to carers below) No impact
4.3 Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4 Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). No impact
4.5 Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment) No impact
4.6 Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people).

No impact
4.7 Religion or belief (Consider impact on people with different religions, beliefs or no belief) No impact
4.8 Marriage and Civil Partnership No impact
4.9 Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities). No impact
4.10 Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation). No impact
4.11 Additional significant evidence (See Guidance Note) Give details of any evidence on other groups experiencing disadvantage and barriers to access due to: • socio-economic status • location (e.g. living in areas of multiple deprivation) • resident status (migrants) • multiple discrimination • homelessness No impact
5. Action planning for improvement (See Guidance Note) Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.
Sign off
Name and signature of person who carried out this analysis
Date analysis completed
Name and signature of responsible Director
Date analysis was approved by responsible Director

7.2 Implementation Plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	Awareness of Policy	Launch of Policy shared at Stand Up	RH	March 20	April 20	Time on agenda
Staff	Access to policy	Upload on to Hub	RH	March 20	April 20	Comms support