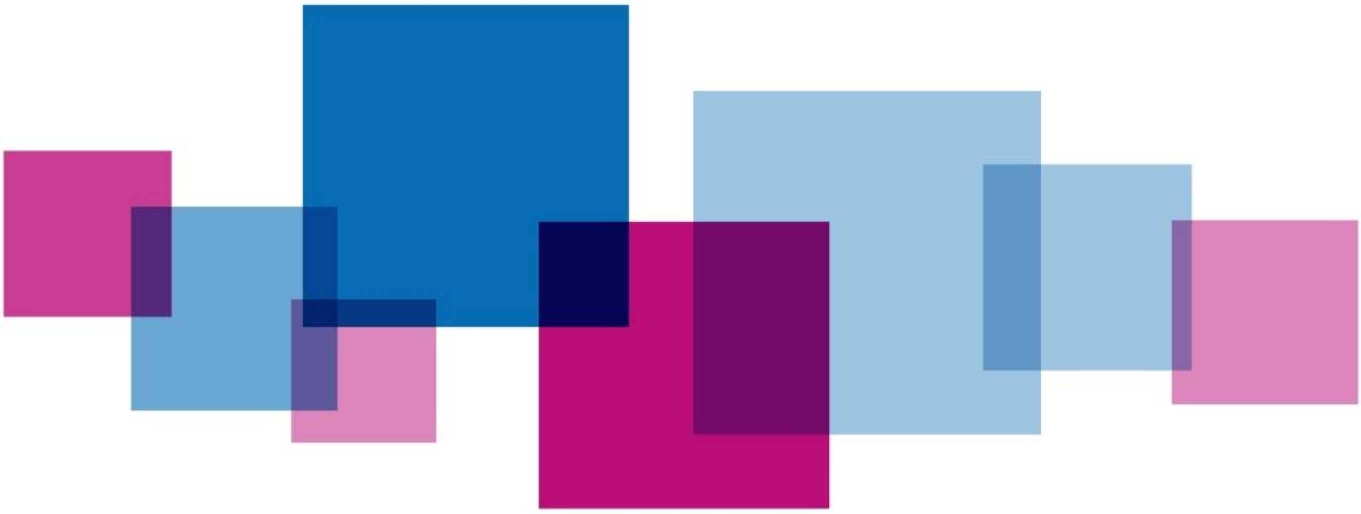
NHS

Bristol, North Somerset
and South Gloucestershire
Clinical Commissioning Group

Clear Screen & Desk 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:	49
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

***Please note that headings were changed to accommodate policy**

Clear Screen & Desk Policy

1. Introduction

1.1. Information Security Management System

The objective of Information Security Management 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

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)

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

Acceptable Use of IT 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.

This policy should also be read in conjunction with the CCG’s Hotdesk Policy.

1.2. Document Purpose

This document provides the detailed policy statements for keeping desks and screens clear of sensitive printed and electronic matter that support the overall IT security objectives of Bristol North Somerset and South Gloucestershire Clinical Commissioning Group (BNSSG CCG) as set out in the security statement in the ISMS.

2. Purpose and scope

2.1. Policy Overview

This policy defines how desks should be kept clear of sensitive printed material and screens should not display sensitive material or be left unlocked when unattended

2.2. Policy Audience

This policy applies to all BNSSG CCG employees including temporary staff, sub-contractors, third party contractors and customers with access to BNSSG CCG information and information systems and services. The reference to desks includes any place where printed material containing confidential data or information that is being, or has been worked upon (eg. BNSSG CCG office, site or home desk area).

Everyone working in or for the NHS has the responsibility to use information and data in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This information sets out the key principles and main 'do's and don'ts' that everyone should follow to achieve this for both electronic and paper records.

The common law duty of confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or court order requirement to do otherwise.

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data

	(f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to BNSSG CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

2.3. Clear Desk Policy Detail

When leaving a desk for a short period of time, users must ensure printed matter containing information that is sensitive or confidential is not left in view.

When leaving a desk for a longer period of time / overnight, users must ensure printed matter containing confidential information is securely locked away. Whiteboards and flipcharts should be wiped / removed of all confidential information when finished with.

2.4. Clear Screen Policy Detail

When leaving the workstation for any period of time, the user must ensure they lock their computer session to prevent un-authorised access to the network and stored information.

All users must ensure their screens cannot be overlooked by members of the public, or people without the necessary authority when confidential data and/or information is displayed. Where appropriate, privacy filters should be used protect the information or alternatively, relocate to a more appropriate place.

Following a period of inactivity, the session will be automatically locked as a failsafe measure.

2.5. Policy Non-Compliance

As with any abuse of BNSSG CCG information, breach of this policy could result in disciplinary action.

3. Review of Policy

3.1. Review Timetable

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

4. 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.

5. Appendices

5.1. Equality Impact Assessment

1 What is it about? ***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Confidentiality and Safe Haven Policy details how BNSSG CCG will meet its legal obligations and NHS requirements concerning confidentiality, information security standards and operates such procedures ensuring that confidential information sent to or from BNSSG CCG is handled in such a way as to minimise the risk of inappropriate access or disclosure. For the purposes of this policy, where Personal or Special Categories of Data are described this will include data that is owed a duty of confidentiality under the Common Law.
b) Who is it for? All staff
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the confidentiality of information to be of equal status across all groups of people.
d) What are the barriers to meeting this potential? There are no barriers.
2 Who is using it? ***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if

possible
The policy is applicable to all.

b) How have you/can you involve your patients/service users in developing the proposal/policy?
Patients and service users have not been involved in developing the policy as this is an operational policy.

c) Who is missing? Do you need to fill any gaps in your data?
There are no gaps.

3 Impact ***Consider how it affects different dimensions of equality and equality groups***

Using the information from steps 1 & 2 above:

a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is?
It is not anticipated that any adverse impact will be created.

b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified?
This is not applicable.

c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups?
This policy is equal across all groups.

d) Is further consultation needed? How will the assumptions made in this analysis be tested?
No.

4 So what (outcome of this EIA)? ***Link to the business planning process***

a) What changes have you made in the course of this EIA?
None.

b) What will you do now and what will be included in future planning?
Not applicable.

c) When will this EIA be reviewed?
At policy review.

d) How will success be measured?
No equality issues are created.

Name of person leading this EIA:	Date completed: Proposed EIA review date:
Signature of director/decision-maker Name of director/decision-maker	Date signed

5.2 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