South, Central and West
Commissioning Support Unit

Clear Screen & Desk Policy

Version 3

South, Central and West Commissioning Support Unit

July 2018

DOCUMENT CONTROL

Document Name	Version	Status	Author
Clear Screen & Desk Policy	*3*	*Final*	*Cyber Security Manager*
Document objectives:	*The objective of this policy is to reduce the risks of unauthorized access to, or loss of, or damage to, information.*		
Target audience:	*All staff*		
Committee/Group Consulted*:*	*SCW Information Governance Steering Group*		
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*		
Training/resource implications:	*All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate IT policies pages*		
Approved and ratified by:	*SCW Information Governance Steering Group SCW Corporate Governance Assurance Group*	*Date: 24 July 2018*	
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*	
Date issued:	*24 –Jul-2018*		
Review date:	***July 2019***		
Author:	*Cyber Security Manager*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
20/11/2015	Cathy Jukes	0.1		Draft
20/11/2015	Cathy Jukes	0.2		Final review prior to formal sign off
02/02/2106	Cathy Jukes	1.0		Updated following approval (added to corporate template)
08/09/2016	Arif Gulzar	1.1		Updated policy review date
04/10/2016	Arif Gulzar	1.1		Signed off by Information Governance Steering Group
29/11/2016	Arif Gulzar	2.0		Reset version after ratification from Corporate Governance Assurance Group
14/12/2017	Arif Gulzar	2.1		Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group
14/05/2018	Arif Gulzar	2.2	All	Updated corporate policy template with corporate branding. Some minor changes and updated section 2.2 with definition of 'sensitive information' aligned with GDPR.
21/05/2018	Arif Gulzar	2.3		Policy reviewed and signed off by IT senior Leadership Team
24/07/2018	Arif Gulzar	3.0		Version changed after CGAG ratification

Reviewers/contributors

Name	Position	Version Reviewed & Date
Simon Sturgeon	Director of IT Services	V2.2 21/05/18
Andy Ferrari	Associate Director of IT Strategy and Planning	V2.2 21/05/18
Cathy Jukes	Associate Director of IT Projects and Programmes	V2.2 21/05/18
Michael Knight	Associate Director of Technology Management and Architecture	V2.2 21/05/18
David Walch	Head of IT Service Delivery	V2.2 21/05/18
Stephanie Wilson	Head of Service Development and Support	V2.2 21/05/18

Version Number: 3.0	Issue/approval date: 24-July-18
Status: Final	Next review date: July 2019

CONTENTS

Version Number: 3.0	Issue/approval date: 24-July-18
Status: Final	Next review date: July 2019

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

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 NHS South, Central and West CSU (SCW) as set out in the security statement in the ISMS.

2. CLEAR SCREEN & DESK POLICY

2.1. Policy Overview

This policy defines how desks should be kept clear of sensitive printed material.

2.2. Policy Audience

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

Confidential information includes

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 SCW CSU 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 considered 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.

Following [up to a maximum of] 15 minutes of inactivity, the session will be automatically locked as a failsafe measure.

2.5. Policy Non-Compliance

As with any abuse of SCW 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 SCW senior management team.

APPENDIX A - EQUALITY IMPACT ANALYSIS

On Clear Screen and Desk Policy

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 SCW 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 SCW 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.

Sign-off

Name of person leading this EIA: **Arif Gulzar**	Date completed: **24-07-2018** Proposed EIA review date: **01-07-2019**
Signature of director/decision-maker **Simon Sturgeon** Name of director/decision-maker **Simon Sturgeon**	Date signed **24-07-2018**

End of Policy Document

Version Number: 3.0	Issue/approval date: 24-July-18
Status: Final	Next review date: July 2019