,

North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

Clear Screen and Desk Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Catherine Jukes – Associate Director of IT Projects and Programmes
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Review date:	25/05/2018
Target audience:	All NHS South, Central and West CSU staff

Document Control Sheet

Title	**IT Services Clear Desk & Screen Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Catherine Jukes
Date Created	14/08/2012
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
0.1	20/11/2015	Cathy Jukes	Draft
0.2	20/11/2015	Cathy Jukes	Final review prior to formal sign off
1.0	02/02/2106	Cathy Jukes	Updated following approval (added to corporate template)
1.1	08/09/2016	Arif Gulzar	Updated policy review date
1.1	04/10/2016	Arif Gulzar	Signed off by Information Governance Steering Group
2.0	29/11/2016	Arif Gulzar	Reset version after ratification from Corporate Governance Assurance Group
2.1	14/12/2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	Title and contact
Philip Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1 Introduction

1.1 Information Security Management

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, contractors and third parties with access to SCW information and information systems and services. The reference to desks includes any place where printed material containing sensitive data is being, or has been worked upon (i.e. SCW office, site or home desk area).

Sensitive information includes business sensitive data (i.e. building plans, financials) not just information that is personally identifiable.

2.3 Clear Desk Policy Detail

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

When leaving a desk for a longer period of time / overnight, users must ensure printed matter containing sensitive information is securely locked away.

Whiteboards and flipcharts should be wiped / removed of all sensitive 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 and/or sensitive 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.