NHS
West Hampshire
Clinical Commissioning Group

CLEAR SCREEN AND DESK POLICY

Version 3.2

Subject and version number of document:	Clear Screen and Desk Policy Version 3.2
Serial number:	COR/044/V3.2
Operative date:	1 October 2019
Author:	CSU Cyber Security Manager
CCG owner:	Senior Information risk Owner
Links to other policies:	
Review date:	September 2021
For action by:	All Staff
Policy statement:	The objective of this policy is to reduce the risks of unauthorised access to, or loss of, or damage to, information.
Responsibility for dissemination to new staff:	Line managers at induction.
Mechanisms for dissemination:	All new and revised policies are promoted through the staff newsletter and intranet, and published on the CCG website.
Training implications:	All staff should be made aware of where to find CCG policies at induction.
Resource implications	There are no resource implications in relation to this policy.
Further details and additional copies available from:	Website: https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Equality analysis completed?	This policy has been assessed by the CCG Equality and Diversity Manager as having a low impact on people with characteristics protected by the Equality Act. As such a full Equality Impact Assessment is not required.
Consultation process	CSU IT Senior Leadership Team, CSU Corporate Governance Assurance Group CCG Policy Sub Group
Approved by:	Policy Sub Group
Date approved:	11 September 2019

Website Upload:

Website	Location in FOI Publication Scheme	https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Keywords:	*Insert helpful keywords (metadata) that will be used to search for this document on the intranet and website*	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	Dec 16		Re-badged as CCG policy.	Nov 16
2	Nov 17		Minor amendments throughout to reflect that this is now a CCG corporate policy.	Nov 17
3	Aug 18	Throughout	Annual review. Amendments in light of GDPR. CCG policy based on CSU policy version 3. Re-formatted into CCG policy format.	Aug 18
4	Sept 19	9 and 11	Annual review. CCG policy based on CSU policy version 3.2 – version control brough in line with that of CSU. Additional statement in section 2.4 re sharing screens when in webinar call, regular review biennial rather than annual.	Sept 19
5				

Review Log:
Include details of when the document was last reviewed:

Version Number	Review Date	Reviewer	Ratification Process	Notes
1.01	Sept 16	CSU IT	Policy Sub Group / Board November 2016	No amendments to content
1.02	Sept 17	CSU IT	Policy Sub Group / Board November 2017	See amend 2 above.
2.00	Aug 18	CSU Cyber Security Manager	Policy sub Group	See amend 3 above
3.02	Sept 19	As above	SCW CSU IT Senior Leadership Team, IG Steering Group and Corporate Governance Assurance Group. CCG Policy Sub Group.	See amend 4 above

CLEAR SCREEN AND DESK POLICY

SUMMARY OF KEY POINTS TO NOTE

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

- When leaving a desk for a short period of time, users must ensure printed matter containing confidential information 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.
- When leaving the workstation for any period of time, the user must ensure they lock their computer session.
- 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 to protect the information.

CLEAR SCREEN AND DESK POLICY

Contents

CLEAR SCREEN AND DESK POLICY

1. INTRODUCTION AND PURPOSE

1.1 Information Security Management

1.1.1 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

1.2.1 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 West Hampshire Clinical Commissioning Group (the CCG) as set out in the CCG's Information Security Management System (ISMS).

2. SCOPE AND DEFINITIONS

2.1 This policy applies to all CCG employees including temporary staff, sub-contractors, contractors and third parties with access to CCG information and information systems and services.

2.2 The reference to desks includes any place where printed material containing confidential data or information is being, or has been worked upon (i.e. CCG office, site or home desk area).

Confidential information

2.3 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.

2.4 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 the 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.

3. CLEAR SCREEN & DESK POLICY

3.1 Clear Desk Policy Detail

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

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

3.1.3 Whiteboards and flipcharts should be wiped / removed of all confidential information when finished with.

3.2 Clear Screen Policy Detail

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

3.2.2 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 to protect the information.

3.2.3 All users are responsible for the information that is displayed on the screens whilst a computer / laptop is being supported remotely by IT service desk or when in a webinar / Skype / WebEX call.

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

3.3 Policy Non-Compliance

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

4. ROLES AND RESPONSIBILITIES

4.1 All staff must adhere to this policy.

5. TRAINING

5.1 There is no formal training available in relation to this policy, however the CCG is required to comply with the CCG information governance staff handbook which stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. As information governance is a framework drawing these requirements together, it is important that staff receive the appropriate training.

5.2 The NHS Operating Framework 'Informatics Planning' and the Data Security & Protection Toolkit training requirement requires that the CCG ensures all staff receives annual basic information governance training appropriate to their role.

5.3 On joining the organisation, CCG staff will receive a copy of the information governance staff handbook and will be required to either sign and return a receipt or send an email to the CSU IG Team to confirm that they have received a copy of the handbook and understand their responsibilities.

5.4 All staff are required to undertake information governance training annually. This should be completed through the E Learning for Health training platform: https://www.e-lfh.org.uk/ (which can be accessed through the ConsultOD Portal) or approved face-to-face information governance training delivered by the information governance team. However, new staff must complete their first training session online. This training includes elements relating to Information Security.

6. EQUALITY ANALYSIS

6.1 The CCG is committed to equality, diversity and inclusion for all, as well as meeting the Public Sector Equality Duty (Equality Act 2010).

6.2 Both new policies, and existing policies when reviewed, come within the Public Sector Equality Duty. This means that policy authors must consider whether the policy will be effective for all patients and / or staff. This process is called equality impact assessment.

6.3 This policy has been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full equality impact assessment is not required.

7. SUCCESS CRITERIA / MONITORING THE EFFECTIVENESS OF THE POLICY

7.1 Compliance with the Data Security and Protection toolkit will be assessed by NHS Digital including a review of evidence, as part of the CCG performance assessment.

7.2 Compliance with / awareness of information governance / IT security will be monitored through the following mechanisms:

- Receipt of the IG Staff handbook confirmation slips or emails confirming staff have received a copy of the handbook and understand their responsibilities
- Completion of induction and annual IG training

- Completion of IG modules / training relevant to the roles of the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, Information Asset Owners and Data Custodians / Information Asset Administrators
- Updates to the West Hampshire CCG IG Group.

8. REVIEW

8.1 This document may be reviewed at any time at the request of either the staff forum or management, or in response to changes in legislation, but will automatically be reviewed on a biennial basis.