

CONTROLLED DOCUMENT

N.B. Colleagues should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

CLEAR DESK, CLEAR SCREEN POLICY

CATEGORY:	Policy
CLASSIFICATION:	Information Governance
PURPOSE:	To ensure both hard-copy information and information viewed on screens is kept secure
CONTROLLED DOCUMENT NUMBER:	BC/IG/005 (replaces BC/IS/009)
VERSION NUMBER:	V002
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	Director of Corporate Services
APPROVED BY:	Executive Team
APPROVED ON:	22 March 2023
IMPLEMENTED ON:	28 April 2023
REVIEW PERIOD:	Every 3 years - unless legislation or best practice changes
REVIEW DATE:	Reviewed in August 2025 – to reflect new Executive Team Structure Next full review: April 2026
ASSOCIATED DOCUMENTS:	Data Protection Policy
Essential Reading for:	All colleagues, temporary staff and contractors

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Policy:	Corporate Governance Team, Executive Team
---	--

Document version control:

Date	Version	Amendments made	Amendments Approved by
March 2022	V002	Policy fully reviewed in line with legislative and best practice requirements. Updated to new agreed controlled documents policy format.	SLT
March 2023	-	No updates made	
March 2024	-	No updates made	
July 2025	V003	Updated to reflect new Executive Team structure and adoption of the term colleague for employee	Director of Corporate Services

For the Use of the Corporate Services Team only:

Date added to Register:	August 2025
Date Published on the Hub:	August 2025
Does it need to be published on website:	No

Registered charity no: 201555 | Registered company no: 601847 | Care Quality Commission registration no: CRT1-579008632 | Homes England registration no: LH0269. Head Office - Prospect Place, Whitehall, Bristol, BS5 9FF.

CONTENTS

- 1. POLICY STATEMENT4
- 2. AIM OF THE POLICY AND RELATED LEGISLATION4
- 3. SCOPE OF THE POLICY4
- 4. DEFINITIONS.....5
- 5. KEY PRINCIPLES AND REQUIREMENTS5
- 6. ROLES AND RESPONSIBILITIES5
- 7. EQUALITY AND DATA PROTECTION7
- 8. IMPLEMENTATION AND TRAINING7
- 9. MONITORING AND REVIEW7

1. POLICY STATEMENT

- 1.1 Brunelcare is committed to the development of secure policies and practices, and in doing so, has implemented this Clear Desk, Clear Screen Policy to increase physical security at Brunelcare locations.
- 1.2 This policy ensures that confidential information and sensitive materials are stored safely and out of sight when they are not in use or when the workspace is vacant.
- 1.3 This policy sets out the basic requirements for keeping a clean workspace, where sensitive and confidential information about Brunelcare employees (colleagues), clients, vendors, and intellectual property is secured.

Signed on behalf of Brunelcare:



Graham Russell
Chair of the Board



Oona Goldsworthy
Chief Executive

2. AIM OF THE POLICY AND RELATED LEGISLATION

- 2.1 The purpose of this policy is to define rules to prevent unauthorised access to personal data and confidential information throughout Brunelcare, as well as to shared facilities and equipment.
- 2.2 For the avoidance of doubt, if a valid data processing agreement is in place between Brunelcare and one of its data processors this policy will apply to said data processor.

Legislative and Legal requirements:

[Data Protection Act 2018](#)

[Freedom of Information Act 2000](#)

[UK GDPR](#)

[ISO 27001 standard, Annex 11.1](#)

[CQC Guidance](#)

3. SCOPE OF THE POLICY

- 3.1 All personal and otherwise confidential internal data processed by Brunelcare is within the scope of this policy unless the data is unambiguously suitable for public dissemination. It also applies to any other sensitive or restricted information even if this may not include personal data.
- 3.2 This policy does not apply to a customer's personal data within that person's home, e.g. a customer's care plan may be left in the individual's home if this has been agreed with the customer or their representative.

4. DEFINITIONS

- 4.1 *'Personal data'* is information that relates to an identified or identifiable individual.
- 4.2 *'Internal data'* refers to any information that is only intended for authorised users and that may be sensitive in nature, for instance a draft budget.

5. KEY PRINCIPLES AND REQUIREMENTS

- 5.1 The objective of the Clear Desk, Clear Screen Policy is to prevent unauthorised access to sensitive personal and/or confidential information.
- 5.2 A clear desk will only contain: a telephone, computer, keyboard, mouse and mat or docking station for laptops and stationery.
- 5.3 When not in use, all information will be locked away in a department cupboard or filing cabinet and the keys kept secure.
- 5.4 Computer screens used to view sensitive and personal data will be sited to prevent them from being overlooked by unauthorised individuals.
- 5.5 Computer terminals will not be left logged on when unattended, and should always be passphrase protected.
- 5.6 Mass storage devices such as CD, DVD, USB drives, or external hard drives will be treated as sensitive material and locked away when not in use.
- 5.7 All computers accessing the Charity's network will be configured to automatically invoke a screen-lock after 10 minutes or less of inactivity. Users should not disable or extend the screen saver timeout period. When leaving their desk, users should lock their computer screen to prevent unauthorised individuals viewing information.
- 5.8 All mobile devices accessing the network will be configured to automatically invoke a screen-lock after 5 minutes or less of inactivity. The device also requires protection with a pin code, or fingerprint authentication.
- 5.9 Printed materials must be immediately removed from printers or fax machines once printed or sent. Printing physical copies should be reserved for when this is necessary. Documents will be viewed, shared and managed electronically whenever possible.
- 5.10 All sensitive documents and restricted information will be placed in the designated shredder bins for destruction once no longer required.
- 5.11 Whiteboards and similar carriers containing information that falls within the scope of this policy will need to be erased once used and flip chart papers may need to be disposed within the confidential waste bins.
- 5.12 Users are not to work on sensitive or personal data in public places where data is likely to be viewed, unless this is required by their role, or users have been specifically authorised to do so.

6. ROLES AND RESPONSIBILITIES

Board

- 6.1 It is the responsibility of the Board to ensure that Brunelcare's policies and procedures reflect statutory requirements and best practice.
- 6.2 The Chief Executive Officer has overall responsibilities for compliance with data protection legislation as delegated by the Board.

Chief Executive Officer

- 6.3 The Chief Executive Officer is responsible for ensuring that the Charity complies with the statutory and good practice requirements governing information use outlined in this policy and is supported by the delegated management responsibilities outlined below.

Director of Corporate Services

- 6.4 The Director of Corporate Services has been delegated responsibility for ensuring organisational compliance with the Data Protection Laws, and is supported by the Data Protection Officer.
- 6.5 The Director of Corporate Services is responsible for ensuring that any substantive changes made to the policy will be communicated to all relevant personnel.

Data Protection Officer

- 6.6 The Data Protection Officer will jointly monitor the effectiveness of this policy and carry out regular reviews.
- 6.7 The Data Protection Officer has delegated responsibility for investigating breaches and non-compliance relating to Information Governance and for providing updates on investigations to the Senior Leadership Team.

Senior Leadership Team and Managers

- 6.8 The Executive Team and Managers are responsible for implementing this policy within their departments and ensuring that staff comply with it.
- 6.9 Managers are responsible for ensuring good security practices are implemented and maintained within their area of responsibility by:
 - 6.9.1 Ensuring colleagues know what is expected of them and that they act in a sensible way to protect information (whether manual or electronic).
 - 6.9.2 Ensuring that policies, guidance and procedures are followed at all times.
 - 6.9.3 Setting a good example to colleagues by applying good security principles to their own work.
 - 6.9.4 Ensuring new starters to the organisation complete the statutory and mandatory training which includes the sign off of reading and understanding the Clear Desk, Clear Screen Policy.
 - 6.9.5 Ensuring departments and colleagues share information only on 'need to know' principles.
 - 6.9.6 Ensuring that regular clear desk, clear screen checks take place.

Colleagues

- 6.10 Colleagues should ensure they have read and understood the policy and ensure it is adhered to.

- 6.11 Colleagues should safeguard and maintain the confidentiality of information they access, create, receive, control or destroy at all times.
- 6.12 Colleagues who leave sensitive, confidential or personal identifiable data on their desk overnight or for lengthy periods will be reminded of their responsibilities by their Line Manager. Persistent offenders may face investigation and disciplinary action.
- 6.13 All colleagues are required to accept personal responsibility for compliance.

7. EQUALITY AND DATA PROTECTION

- 7.1 Brunelcare seeks to embed an environment where all clients, visitors and colleagues are treated as individuals, fairly and in a consistent way. The Charity works within the spirit and the practice of the Equality Act 2010 by promoting a culture of respect and dignity and actively challenging discrimination, should it ever arise. This Policy will be applied in a way that is consistent with these principles.

Data Protection

- 7.2 Brunelcare is committed to ensuring protection of all personal information that it holds, and to provide and protect all such data.
- 7.3 Brunelcare is dedicated to safeguarding the personal information under the Charity's control and in maintaining a system that meets our obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. The Charity's practice related to data protection is set out in Brunelcare's Data Protection Policy.

8. IMPLEMENTATION AND TRAINING

- 8.1 Brunelcare will establish effective arrangements for communicating the requirements of this policy. This will include all new starters being informed on the requirements of this policy as part of their induction to Brunelcare.

9. MONITORING AND REVIEW

- 9.1 The implementation of this policy, and the effectiveness of the arrangements detailed within it, will be monitored by the Director of Corporate Services.
- 9.2 Regular and ongoing Clear Desk, Clear Screen checks will be undertaken to ensure continued compliance with this policy. These checks may be initiated by Brunelcare's Data Protection Officer but are normally to be conducted by site or line managers.
- 9.3 Where a weakness has been identified, the auditor must email that colleague with text along the following lines:

*We conducted an audit on **[date, time]** and found the following weakness: **[e.g. service user files left on desk.]** This is classed as a breach of our [Clear Desk, Clear Screen policy](#). (available on BORIS)*

Leaving personal or otherwise sensitive data unattended may potentially provide unauthorised access to this data. Please always ensure that unsupervised data is locked away or passphrase protected.

Please note: this incident has been logged. Persistent breaches of the policy may lead to additional training requirements or may be regarded as a disciplinary incident. Please contact the Brunelcare Data Protection Officer or myself if you feel that the above mentioned incident did not leave data vulnerable to potential unauthorised access, or if you feel that you are not given adequate resources to adhere to Brunelcare's Clear Desk, Clear Screen Policy.

- 9.4 This policy will be reviewed by the Director of Corporate Services to ensure it remains fit for purpose and complies with any changes to the relevant Information Governance law.