



### **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 This is to avoid the risk of out of date printed versions of the document.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.**

## **SMARTPHONE AND MOBILE DEVICE POLICY**

<b>CATEGORY:</b>	Policy
<b>CLASSIFICATION:</b>	Information Governance
<b>PURPOSE:</b>	To ensure the safe use of smartphones and mobile devices which Brunelcare supplies to its employees
<b>CONTROLLED DOCUMENT NUMBER:</b>	BC/IG/003
<b>VERSION NUMBER:</b>	V003
<b>CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:</b>	Director of Corporate Services
<b>CONTROLLED DOCUMENT AUTHOR:</b>	Director of Corporate Services
<b>APPROVED BY:</b>	Senior Leadership Team
<b>APPROVED ON:</b>	20 July 2022
<b>IMPLEMENTED ON:</b>	February 2023 (version V002) September 2025 (version V003)
<b>REVIEW PERIOD:</b>	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
<b>REVIEW DATE:</b>	Latest Review Date: September 2025 – to reflect new Executive Team Structure Next full review date February 2026
<b>ASSOCIATED DOCUMENTS:</b>	Data Protection Policy Bring Your Own Device To Work Policy Acceptable Use Policy
<b>Essential Reading for:</b>	All employees and temporary staff

## Document Consultation and Review Process

<b>Groups/Individuals who have overseen the development of this Policy:</b>	<b>Corporate Governance Team, Senior Leadership Team</b>
---	--

## Document version control:

<b>Date</b>	<b>version</b>	<b>Amendments made</b>	<b>Amendments Approved by</b>
June 2022	V001	New policy	SLT
February 2023	V002	Minor updates and formatting	Head of Corporate Governance
September 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:

<b>Date added to Register:</b>	<b>July 2022</b>
<b>Date Published on the Hub :</b>	<b>February 2023 (V002) September 2025 (V003)</b>
<b>Does it need to be published on website:</b>	<b>No</b>

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.



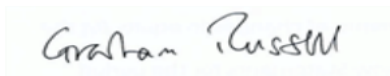
# CONTENTS

- 1. POLICY STATEMENT ..... 5
- 2. AIM OF THE POLICY AND RELATED LEGISLATION ..... 5
- 3. SCOPE OF THE POLICY ..... 6
- 4. DEFINITIONS..... 6
- 5. KEY PRINCIPLES AND REQUIREMENTS ..... 6
- 6. ROLES AND RESPONSIBILITIES ..... 7
- 7. EQUALITY AND DATA PROTECTION ..... 8
- 8. IMPLEMENTATION AND TRAINING ..... 9
- 9. MONITORING AND REVIEW ..... 9

## 1. POLICY STATEMENT

- 1.1 Modern smartphones and mobile devices, such as tablets, are capable of accessing and storing data, and running business applications. It is recognised that whilst the use of smartphones can bring many benefits, and help employees to perform in their jobs, it also introduces a significant risk that data, or access to that data, may fall into the wrong hands due to the loss or improper use of a smartphone.
- 1.2 Brunelcare is committed to ensuring that data is not put at risk from the use of smartphones or mobile devices. For those employees with a business requirement to access the organisation's data with a smartphone or mobile device, this policy provides the necessary guidance so that it is done in a manner that does not introduce unacceptable threats to the safety and integrity of this data.
- 1.3 Brunelcare expects all employees using a smartphone or mobile device as part of their role to follow this policy at all times.

**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 provide effective controls to ensure that an employee's access to the organisation's data and any information systems using a smartphone or mobile device is authorised, secure and confidential and in line with the charity's business requirements.
- 2.2 This policy has been developed to ensure the remote processing of our data is operated in accordance with statutory requirements and all relevant guidance.
- 2.3 This policy will ensure that any risks associated with smart phone based access are recognised, assessed and managed.

### **Legislative and Legal requirements:**

[Data Protection Act 2018](#)  
[Freedom of Information Act 2000](#)  
[General Data Protection Regulation \(GDPR\)](#)  
[Protection from Harassment Act 1997](#)  
[Communications Act 2003](#)  
[Road Vehicles \(Construction and Use\) Regulations 2003](#)

### 3. SCOPE OF THE POLICY

- 3.1 This policy applies to all employees who have been issued with a smartphone or mobile device as part of their employment.
- 3.2 The IT Team maintains a list of employees who have been given access to a smart phone or mobile device.

### 4. DEFINITIONS

- 4.1 '*Personal Data*' refers to information that relates to an identified or identifiable individual, as defined by the Data Protection Act 2018 and the GDPR. See further the organisation's Data Protection Policy.
- 4.2 A '*smartphone*' is a mobile phone that allows users to connect to the internet, store information, use email and install programs.
- 4.3 A '*mobile device*' is a piece of portable electronic equipment (e.g. a tablet) that can connect to the internet, store information, use email and install programs.
- 4.4 A '*user*' is identified as any employee who has been issued with a smartphone and authorised to access our IT systems and networks remotely.
- 4.5 '*Encryption*' refers to the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing the key. The result of the process is encrypted information. Password protection alone is not a form of encryption.

### 5. KEY PRINCIPLES AND REQUIREMENTS

- 5.1 Employees will be issued with a smartphone and/or mobile device should there be a business requirement due to their job role. The smartphone or mobile device will be requested by their Line Manager via the IT Team.
- 5.2 All smart phones and mobile devices will be held and transported securely and not be left unattended (e.g. in vehicles). All devices should be locked away when not in use.
- 5.3 Stolen or lost equipment must be reported as soon as possible to the IT Team; [helpdesk@brunelcare.org.uk](mailto:helpdesk@brunelcare.org.uk).
- 5.4 Users may not install any unauthorised or unlicensed software on any Brunelcare issued smartphones or mobile devices.
- 5.5 Brunelcare issued smart phones or devices should not be used for non-business-related purposes.
- 5.6 Brunelcare issued smart phones or mobile devices will only be used by the individual that they have been issued to. Employees may not share the device with or lend it to anyone else, for example a family member or work colleague, even for temporary access to a non-work-related app or service.
- 5.7 Personal information should only be remotely accessed, held and processed on smart phones or mobile devices supplied, authorised or approved by Brunelcare.

- 5.8 Employees are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems. Smartphone or mobile device screens will be locked when not actively being used.
- 5.9 The use of smart phones or mobile devices in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of equipment.
- 5.10 Employees must ensure that Brunelcare issued smart phones, mobile devices and information accessed at home are secure from theft and damage and cannot be accessed by family members, friends or any other unauthorised user.
- 5.11 Data will not be held on a smartphone or mobile device for longer than it is required and should be deleted or archived promptly, in line with the organisation's data retention and disposal policy, to reduce the risk of the data being accessed by the wrong person.
- 5.12 Personal information will not be stored on an unencrypted device (password protection alone is not a method of encryption and must not be relied upon as such).
- 5.13 Emails containing personal information and other Charity related information must not be sent to or from personal email accounts.
- 5.14 Employees will use smartphones and mobile devices in line with the organisation's code of practice around computer use and the Acceptable Behaviour Policy. As such, employees will not use smartphones and devices provided by the organisation for:
- Private use, such as accessing personal social media accounts.
  - Inappropriate use, such as accessing services or content of an illegal, pornographic or violent nature.
  - Leaving voice messages or sending text messages that are of a threatening or abusive nature.
- 5.15 Employees will adhere to the law and best practice related to using a smartphone or mobile device whilst driving. See further Brunelcare's Driving at Work Safely Policy.

## **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.

### **Chief Executive Officer**

- 6.2 The Chief Executive Officer has overall responsibilities for compliance with data protection legislation which is delegated by the Board.
- 6.3 The Chief Executive is responsible for ensuring that the organisation complies with the statutory and good practice requirements governing smartphone and mobile device 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 to ensure that the organisation has robust data protection processes in place that comply with current legislation and best practice guidance.

### **Head of Digital Systems**

- 6.5 The Head of Digital Systems has responsibility for ensuring that adequate technical security controls are in place to meet the requirements of this policy.

### **Senior Leadership Team and Managers**

- 6.6 All Managers are responsible for ensuring that their colleagues receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance.
- 6.7 Managers are responsible for determining eligibility of colleagues and appropriate mobile device(s) for their role.

### **Colleagues**

- 6.8 Colleagues must ensure that they are aware of their responsibilities for complying with smartphone and mobile device use requirements in accordance with this policy and any supporting guidance.
- 6.9 Colleagues with authorised smartphones and/or mobile devices must safeguard equipment and information and report immediately any associated security incidents.
- 6.10 Colleagues are responsible for smartphones and mobile devices and all data held on them. In the event of loss, theft or any data security incidents associated with smart phone or mobile device use, colleagues must inform the IT Team ([helpdesk@brunelcare.org.uk](mailto:helpdesk@brunelcare.org.uk)) and follow the procedure for suspected data breaches including informing the Data Protection Officer and Corporate Services Team.

## **7. EQUALITY AND DATA PROTECTION**

- 7.1 Brunelcare seeks to embed an environment where all clients, visitors and employees 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 data that it holds, and to protect all other confidential data and information.
- 7.3 Brunelcare is dedicated to safeguarding the personal information under the organisation'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



organisation'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:

8.1.1 All new starters being informed on the requirements of this policy as part of their induction to Brunelcare.

8.1.2 Annual training being provided on data protection requirements via the organisation's e-learning system.

## **9. MONITORING AND REVIEW**

9.1 The implementation of this policy, and the effectiveness of the arrangements detailed within it, will be monitored and reviewed by the Director of Corporate Services, with input from the Data Protection Officer and Head of Digital Systems.