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 This is to avoid the risk of out of date printed versions of the document.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

BRING YOUR OWN DEVICE POLICY

CATEGORY:	Policy
CLASSIFICATION:	Information Governance
PURPOSE:	To establishes Brunelcare's guidelines for employee use of personally owned electronic devices for work-related purposes
CONTROLLED DOCUMENT NUMBER:	BC/IG/004
VERSION NUMBER:	V003
CONTROLLED DOCUMENT SENIOR LEADERSHIP TEAM LEAD:	Director of Corporate Services
CONTROLLED DOCUMENT AUTHOR:	Director of Corporate Services
APPROVED BY:	Senior Leadership Team
APPROVED ON:	20 July 2022
IMPLEMENTED ON:	February 2023 (version V002) August 2025 (V003)
REVIEW PERIOD:	Every 3 years - unless changes to legislation, best practice or internal roles and responsibilities
REVIEW DATE:	Latest Review Date: July 2025 – to reflect new Executive Team Structure Next full review date July 2028
ASSOCIATED DOCUMENTS:	Data Protection Policy Smartphone and Mobile Device Policy
Essential Reading for:	All colleagues including temporary/contract staff

Document Consultation and Review Process

Groups/Individuals who have overseen the development of this Policy:	**Corporate Governance Team, Senior Leadership Team**

Document version control:

Date	version	Amendments made	Amendments Approved by
July 2022	V001	New policy	SLT
February 2023	V002	Minor updates and formatting	Head of Corporate Governance
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:	**July 2022**
Date Published on the Hub:	**February 2023 (V002)** **August 2025 (V003)**
Does it need to be published on website:	**No**

CONTENTS

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

1. POLICY STATEMENT

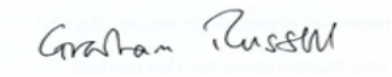
1.1. This policy describes the steps that the organisation and its employees (colleagues) will follow when connecting personal computers and devices to organisation systems and networks.

1.2. 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 colleagues 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.

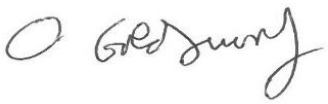
1.3. Brunelcare has taken a decision to allow staff to use their own smartphone or mobile device for work purposes provided this policy has been followed and the device has been authorised for use. This policy has been developed to ensure that the organisation's data is not put at risk from the use of smartphones in this manner. For those members of staff with a business requirement to access the organisation's data with a smartphone, this policy provides the necessary guidance so that it is done in a manner that does introduce unacceptable threats to the safety and integrity of this data.

1.4. Brunelcare expects all colleagues using their own 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 This policy outlines requirements for Bring Your Own Device (BYOD) usage and establishes the steps that both users and the Digital Services department will follow to initialise, support, and remove devices from company access.

2.2 The purpose of the policy is to provide effective controls to ensure that colleague access to the organisation's data and any information systems through the use of a smartphone is authorised, secure and confidential, in line with our business requirements and that remote processing of our data is operated in accordance with Brunelcare policy, statutory requirements and all relevant guidance.

2.3 The aim of the policy is to 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)

3. SCOPE OF THE POLICY

3.1 Equipment covered by this policy includes (but is not limited to):

- Desktops, laptops, and tablet computers.
- Smartphones (defined as any cellular telephone that connects to the internet via Wi-Fi or a mobile provider network).
- Flash, memory, and/or thumb drives.
- External hard disks.
- iPods, iTouches, and similar entertainment and portable music devices that connect to WiFi networks.
- Entertainment and gaming consoles that connect to Wi-Fi networks and are used to access organisation email and systems.
- Wearable devices such as watches, VR headsets, and augmented reality glasses with WiFi or Bluetooth.

4. DEFINITIONS

4.1 '*Personal data'* covers 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 colleague 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.

4.6 '*Bring Your Own Device (BYOD)'* is the term used to describe the approach of letting colleagues use their own mobile device for work purposes. For example, the organisation may allow colleagues to use their own smartphones to access work email while out of the office, rather than supplying corporate owned devices for that specific task.

4.7 The '*Mobile Device Management (MDM) Service'* refers to the service that allows an organisation to remotely control, monitor and enforce policies on colleagues mobile devices. This lets an organisation ensure that the devices meet required compliance to protect any data that may be processed by or stored on the device.

5. KEY PRINCIPLES AND REQUIREMENTS

5.1 Only personal devices authorised by the organisation's Digital Services department will be allowed to access organisation data in line with this policy.

5.2 For a colleague to obtain authorised and secure smartphone access to the organisation's data an MDM service will be used, where possible, and the user issued with instructions for enrolling onto the organisation's MDM service. The Digital Services Team will ensure the user completes this process and registers their device as one being used for employment purposes.

5.3 Having obtained the required authorisation, a user must enrol their device in our MDM, where possible, before they can access any organisation data or use their device for work purposes. If the device does not meet required specifications for safe use, the user does not agree for it to be enrolled in the MDM service (where this is available), or disagrees with any of the policies to be applied, then authorisation will not be given for the device to be used for work purposes under this policy.

5.4 Ant technical problems or queries regarding remote access or mobile devices will be addressed to the Digital Services team; helpdesk@brunelcare.org.uk

5.5 A log of all users who are authorised to access the organisation's data on their personal phones will be maintained by the Digital Services department.

5.6 Users will inform their Line Manager when access through their device is no longer required, or when leaving the organisation. This will allow all Brunelcare's data and apps to be deleted from the user's device before it is unenrolled from the MDM service, where this is being used.

5.7 Users are responsible for their device and all data held on it. In the event of loss, theft or any data security incidents associated with the device,colleagues must inform the Digital Services Team (helpdesk@brunelcare.org.uk) and follow the procedure for suspected data breaches, including informing the Data Protection Officer and Corporate Services Team.

5.8 Where available, users may connect their personal smartphone to the organisation's guest wireless network to get internet access.

5.9 Users are responsible for ensuring that unauthorised individuals are not able to see or access the organisation's data or systems via the user's device. Screens should be locked when not actively being used.

5.10 The use of personal devices for accessing the organisation's data or services in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of an unlocked device.

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 organisation related information must not be sent to or from personal email accounts.

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 Services

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

Managers

6.6 All Managers are responsible for ensuring that their teams 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 Digital Services Team (helpdesk@brunelcare.org.uk) and follow the procedure for suspected data breaches including informing the Data Protection Officer and Corporate Services Team via dataprotection@brunelcare.org.uk.

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 organisation 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 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.

8.2 It is mandatory for all new colleagues to undertake data protection training relevant to their role as part of their induction process.

8.3 Any specific training needs identified to ensure compliance with this policy should be referred to the colleague's Line manager.

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 Services.