



iPad: Access for Bank Workers **Standard Operating Procedure**

Contents

1	Scope.....	2
2	Procedure.....	2
3	Responsibilities	4
4	Audit and Review (evaluating effectiveness)	4
5	Associated Documentation	5
6	Financial Checkpoint	5
7	Equality Analysis.....	5
	Appendix A	6

1 Scope

- 1.1. This procedure describes the arrangements and processes relating to Trust issued iPads for use by Bank Workers. This group of staff do not have Corporately Owned Personally Enabled (COPE) issue iPads.
- 1.2. The Trust approved a business case to supply each Operating Unit with a supply of iPads by Bank Workers undertaking ad-hoc operational shifts.
- 1.3. Access to these shared iPads will also be available to permanent Operational staff who are without their iPad while waiting for a replacement due to damage (or for other similar reasons). However, the shared iPad cannot be retained whilst not on duty.
- 1.4. This document defines the safe storage and use of the shared iPads and any regimes which support infection prevention and control.

2 Procedure

2.1 Storage and charging

The iPad will be kept in a locker at the Make Ready Centre or reporting base. The cupboard must be kept locked unless you are withdrawing or returning the iPad. When the iPad is in the locker it must be placed on charge.

For Make Ready Centres (MRC) the iPad lockers, should where possible, be located within the Make Ready areas, or if required due to capacity or logistic reasons located in MRC corridors. For Ambulance stations, the locations of the iPad lockers will be agreed with IT, Operational Management or the Make Ready Centre Manager.

2.2 Withdrawal and return procedure

Access is via a keypad and the combination is available from the Operational Support Desk (OSD). Ensure any personal data or images are deleted before it is returned to the locker as these will not be removed automatically when logging out of the device.

For operational reasons certain sites may need to have a site-specific storage and usage process, please check with the local Duty Manager.

2.3 Use of iPad during shift

At the start of the shift the user must log on to the iPad using their SECamb computer username (firstname.lastname) and password.

Use of the iPad during the shift must follow the same policies and procedures as COPE iPads issued to other staff. Please refer to the Mobile Device Policy, Social Media Policy, and guidance on the use of iPads on the Trust website (The Zone).

At the end of the shift the user must log off the iPad by selecting the user icon (top right-hand corner of the display) and selecting “log out”.

2.4 ePCR

In line with Trust policy, Bank Workers should always endeavour to create an Electronic Patient Care Record (ePCR) on the iPad.

Training will be given by the local OTLs or iPad champions on station.

2.5 Loss or damage reporting process

If you lose or damage an iPad this must be reported on a Datix form and to the IT Service Desk via the Self Service Portal.

You should also inform the Duty Operational Team Leader.

All devices must be visually inspected for damage at the beginning and end of each shift. Damages should be reported immediately via process in 2.5.

2.6 Repeated and/or careless loss of the iPad may be managed under the Capability Policy.

2.7 Infection control and Cleaning of IPADS

The iPad should be cleaned using the correct method according to the Trust Infection Prevention & Control Policy and Procedures.

The iPad cover itself should be cleaned regularly using Clinell wipes to ensure risk of cross contamination is minimised between patient encounters.

The iPad should be regularly sanitised during operational duty, and be also sanitised prior to their return to the locker using Clinell wipes by the operational staff.

Software updates

IT will instruct when the iPad requires an update, this should be done by the Duty OTL or iPad 'Super-Users' when the iPad is not in operational use.

In the event of an iPad failure, a replacement or repair should be sought via the Self-Service Portal or by calling 0300 123 5520 and reported on the DATIX system and also to your OTL.

iPads remain the property of the Trust

3 Responsibilities

- 3.1 The **Chief Executive Officer** is responsible for patient safety
- 3.2 The **Medical Director** is responsible for clinical practice in the Trust.
- 3.3 **Operating Unit Managers/Operations Managers** are responsible for ensuring Bank workers have access to sharing iPads.
- 3.4 **Bank Workers** are responsible for maintaining, cleaning, and checking the sharing iPad issued to them on a shift basis and ensuring that they have them available whilst on duty.
- 3.5 **The Operational Team Leaders** are responsible for managing and implementing the procedure, and for monitoring and auditing the process, including annual reports to the Trust.

4 Audit and Review (evaluating effectiveness)

- 4.1 All procedures have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.
- 4.2 Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).
- 4.3 This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.
- 4.4 All changes made to this procedure will go through the governance route for development and approval as set out in the Policy on Policies.

5 Associated Documentation

Social Media Policy

Mobile Device Policy

Infection Prevention and Control Policy

Infection Prevention Ready Procedure

Disciplinary Policy and Procedure

Capability Policy and Procedure

6 Financial Checkpoint

- 6.1 To ensure that any financial implications of changes in policy or procedure are considered in advance of document approval, document authors are required to seek approval from the Finance Team before submitting their document for final approval.
- 6.2 This document has been confirmed by Finance to have financial implications and the relevant Trust processes have been followed to ensure adequate funds are available.

7 Equality Analysis

- 7.1 The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.
- 7.2 Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature, then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.

Appendix A

Bank iPad sign in and out form

Name (Print)	Date	Sign out iPad	Time	Sign in iPad (Ensure you have logged out).	Time	Sanitised before storage Y/N	Signature
			:		:		
			:		:		
			:		:		
			:		:		
			:		:		
			:		:		
			:		:		