THE STATE HOSPITALS BOARD FOR SCOTLAND

MOBILE DEVICE POLICY

Policy Reference Number	IG21	Issue: 2
Lead Author	Information Technology Security Officer	
Contributing Authors	Short Life Working Group (SLWG) Mobile Devices	
Advisory Group	IT Sub Group	
Approval Group	Policy Approval Group (PAG)	
Implementation Date	4 October 2022	
Next Review Date	4 October 2025	
Accountable Executive Director	Director of Finance and eHealth	

The date for review detailed on the front of all State Hospital policies/ procedures/ guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/ procedure/ guidance at any time due to organisational/ legal changes.

Staff are advised to always check that they are using the correct version of any policy/ procedure/ guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies/ procedures/ guidance can be found on the intranet: http://intranet.tsh.scot.nhs.uk/Policies/Policy%20Docs/Forms/Category%20View.aspx

REVIEW SUMMARY SHEET

No changes required to policy (evidence base checked)	☐

Changes required to policy (evidence base checked)	☒

Summary of changes within policy:

October 2022 - review

Alteration to the working in the scope of the policy.

"All devices shall be intended for business use only unless determined, in advance, otherwise." to "All devices shall be intended for business use only unless authorised, in writing in advance, by eHealth Management".

"All devices shall be subject to monitoring, auditing and location tracking, where applicable." to "All devices may be subject to monitoring, auditing and location tracking, where possible. This will be done in accordance with written procedures".

"Users should have no expectation of privacy while in possession of the device." to "Users should have no expectation of privacy when using any mobile device owned and supplied by TSH".

Contents

1. Introduction/Purpose

The Network & Information Systems Regulations 2018 ("NIS Regulations") places legal obligations on the use of mobile devices and teleworking equipment used within The State Hospital (TSH).

This policy advises how TSH can meet some of its legal obligations and requirements under confidentiality, data protection and information security standards. The purpose shall be to ensure the security of mobile devices and any resident data or applications.

This policy should be read in conjunction with the policy SP28 Technology and Electronic devices within the State Hospital Policy and Procedure.

2. Scope

The term mobile devices shall be applicable to any electronic device that is not considered a desktop or laptop computer. It shall include mobile phones, Dictaphones, USB drives, external hard drives, tablet devices (such as iPads) and any other mobile device that could be used for processing or storing organisational data, which is provided by the organisation. All devices shall be intended for business use only unless authorised, in writing in advance, by eHealth management. All devices shall be subject to monitoring, auditing and location tracking, where possible. This will be done in accordance with written procedures. Users should have no expectation of privacy when using any mobile device owned and supplied by TSH.

This policy applies to all staff at TSH that require the use of a mobile device.

3. Mobile Device Policy

3.1 General working practices

Deployment of devices shall require approval from the relevant authority. This shall be in accordance with the published guidance and the relevant documentation, Mobile Device Request Form. This form will be available on the Intranet (Forms/Documents, Online Forms, e-Health) and shall be completed prior to devices being deployed.

Only approved mobile devices should be used for processing or storing organisational data.

All devices shall be encrypted, before deployment, to a level of encryption that is suitable for the device and at a minimum to support the data being processed/stored. For devices that can be used to carry data, in many forms, extra security measures shall be used, such as the use of passphrases.

All authorised users shall ensure that devices are not the primary repository of data, so that if the device is lost or stolen it does not affect service delivery.

Devices are not to be left within public places, be on display within unattended vehicles or have confidential information on display within public areas. Any lost/stolen/damaged equipment shall be reported to the organisation at the earliest opportunity and not exceed more than 48 hours. At weekend/public holidays the report should be submitted at the earliest opportunity.

The security department shall have the right to refuse entry to the hospital of any mobile device issued by the eHealth department. They can also remove any TSH assigned mobile device from any staff member, but shall be required to return the device to the eHealth department.
All devices shall be recorded within the eHealth asset register and shall remain the property of TSH at all times and as such can be recalled when necessary.

3.2 Dictaphones and digital recording equipment

All recordings shall be stored on TSH infrastructure for a predetermined amount of time and shall be accessed by authorised personnel only. All recordings should be for business purposes only unless formally agreed, in writing, in advance

3.3 Mobile Phones and Tablet devices (including smart phones)

eHealth will secure and can monitor the device using appropriate mobile device management controls.

All users shall ensure that devices are only connected to private secure wireless networks when they are not using the devices data connection, where applicable, no public/open/free network connections.

The use of mobile phones and tablet devices abroad will need approval from the eHealth department before being taken.

3.4 Applications for Mobile devices

All apps shall be pre-approved and installed in accordance with the mobile device management controls. Any app not pre-approved shall go through an approval process before being deployed. All apps shall be for business use only.

4. Equality and Diversity

The State Hospitals Board (the Board) is committed to valuing and supporting equality and diversity, ensuring patients, carers, volunteers and staff are treated with dignity and respect. Policy development incorporates consideration of the needs of all Protected Characteristic groups in relation to inclusivity, accessibility, equity of impact and attention to practice which may unintentionally cause prejudice and / or discrimination.

The Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information/documents in alternative formats and are happy to discuss individual needs in this respect. If information is required in an alternative format, please contact the Person-Centred Improvement Lead on 01555 842072.

Line Managers are responsible for ensuring that staff can undertake their role, adhering to policies and procedures. Specialist advice is available to managers to ensure that reasonable adjustments are in place to enable staff to understand and comply with policies and procedures. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

5. Stakeholder Engagement

Key Stakeholders	Consulted (Y/N)
Patients	N
Staff	Y
TSH Board	Y
Carers	N
Volunteers	N

6. Communication, Implementation, Monitoring and Review of Policy

This policy will be communicated to all stakeholders within The State Hospital via the intranet and through the staff bulletin. The IT Sub Group will be responsible for the implementation and

monitoring of this policy. This policy will be reviewed every three years, and when appropriate to take into account changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner's Office.