NHS Shetland

POLICY DOCUMENT

Policy on Mobile / Portable Computing Devices and Data Security

Release: Final

Date Created: 3 March 2009

Owner: David Priest

Compiled by: David Priest

Document Reference: SHB Mobile Protection Policy v2.0

TABLE OF CONTENTS

1 Policy Document History 3
- 1.1 Document Location 3
- 1.2 Revision History 3
- 1.3 Approvals 3

2 Purpose of Document 4

3 Policy 5

4 Appendix A - Application for a Secure Encrypted Memory Stick 7

5 Appendix B - Conditions of Use Policy – (to be signed on receipt of device) 8

1 Policy Document History

1.1 Document Location

The source of this document can be found at:

SHB Mobile Protection Policyv2.0.doc

1.2 Revision History

Date of this Revision: 3rd March 2009

Date of Previous Revisions:

Revision date	Previous revision date	Summary of Changes	Changes marked
24/02/2009	N/A	Final draft.	N/A
03/03/2009	24 February 2009	Update to draft following comments received from frontline.	N/A

1.3 Approvals

This document requires the following approvals:

Name	Signature	Title	Date of Issue	Version
Approved by: Sandra Laurenson on behalf of NHS Shetland Board		Chief Executive	03/03/2009	2.0

2 Purpose of Document

The purpose of the Policy is to define NHS Shetland's requirements on the management and handling of NHS Shetland data.

A mobile / portable computing device is defined as any easily transportable computing device that is capable of storing and transferring data. It applies when the devices are taken outside of NHS Shetland property premises. The procedure refers to all NHS Shetland data.

The policy applies to the following removable media:

- Memory sticks
- Mobile Phones
- CDs and DVDs
- Laptop computers
- Handheld Computers (PDAs) and Blackberry devices
- Digital Imaging and Cameras

3 Policy

3.1 The storage of NHS Shetland data on portable devices, outside of NHS Shetland premises, is prohibited unless special permission has been granted (see sections 3.4& 3.5).

3.2 When not in use, all devices should be securely locked using access passwords where available. Data on individual files or documents should have passwords applied. Devices should not be left in motor vehicles.

3.3 All laptop computers should be switched off and locked securely when not in use. They should be kept only in locked secure premises.

3.4 Staff with a bona-fide need for encrypted secure memory sticks will require to submit an application for use (see the attached conditions of use form). If approved, the staff member will be supplied with a secure memory stick subject to acceptance of the 'conditions of use' statement. Staff are not allowed to use their own memory sticks, only those provided by the NHS Shetland IT department.

3.5 Where the requirement to hold data on mobile devices is integral to the delivery of a service, or enhances the safety of a clinical process, it can only be authorised through the submission of a statement of need authorised by your line manager. Such requests will also be the subject of a risk assessment by the IT Security Officer prior to approval being granted. On approval, the member of staff will be with be authorised to use an encrypted laptop or issued with an NHS Shetland secure encrypted device for use outside of NHS Shetland premises.

3.6 The statement of need will be subject to the following approvals:

a. The appropriate documentation will be authorised by the relevant line manager or head of department.
b. These will be considered by the IT Security Officer and a recommendation on acceptance or otherwise will be made to Assistant Director of Service Improvement (ADSI) or Director of Service Improvement (DSI). Rejected requests will be advised through the Service / Departmental Manager together with a reason for rejection.
c. The Director of Pubic Health, as the Caldicott Guardian will adjudicate where there is any appeal. That decision will be final.

3.7 The procedure reflects NHS Shetland's board intention to ensure that patient and staff identifiable data is kept secure and risks of data or equipment being lost, stolen or accessed by unauthorised persons is reduced. The procedure is in line with Scottish Government CEL 45 (2008), 9/10/08 and the NHS Scotland E-Health Mobile Data Protection Standard (29/9/2008) and will be incorporated into the NHS Shetland Information Security Policy due for revision in 2009. The IT Security Officer will regularly audit requests for access for devices outwith NHS Shetland properties and report to Director of Service Improvement.

4 Appendix A - Application for a Secure Encrypted Memory Stick

Name (please print) :

Designation :

Location :

Signature :

Briefly describe the circumstances in which a memory stick will be used with reference to the service benefits that will derive from its use and the impact of this request not being granted. Please note that applications for non-specific general use will not be considered.

In submitting a request for a secure encrypted memory stick, I am aware of the limitations on its use and will agree to abide by the above 'Mobile Protection Policy'.

Please complete your manager's details as approved applications will be notified to them.

Manager's Name :

Designation :

IT Security Manager's Approval of Request :

5 Appendix B - Conditions of Use Policy – (to be signed on receipt of device)

In accepting an NHS Shetland laptop or secure encrypted memory stick, I accept the conditions set out in the NHS Shetland procedure on mobile / portable computing devices. Specifically:

- I am aware that the device will not be used for the storage of patient, staff or financial identifiable data other than with the explicit permission of the IT Security Officer.
- I will ensure that use of the device and its approved host PC will be restricted to me as the registered device owner.
- I will use the device solely for the purpose for which it has been granted and ensure that data is only held on the device for the period during which it is required.
- I will store the device securely when not in use and ensure that if the device is lost; such loss is reported to the IT Helpdesk, line manager and Director of Service Improvement immediately. A formal incident reporting form GR1 will also need completion.

Name (please print) :

Designation :

Date :

Signature :