London Ambulance Service NHS
NHS Trust

Laptop Security Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: Provides an overview of the London Ambulance Service NHS Trust's approach to Laptop security to ensure that laptops and the information stored on them are secure whilst in use, or in transit.

Sponsor Department: Information Management and Technology (IM&T)

Author/Reviewer: Information Security Manager. To be reviewed by Aug 2011

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
20/02/2008	0.1	Information Security Manager	Initial Draft
04/06/2008	0.2	Head of Records Management; Information Security Manager	Structure and content amendments
12/08/08	0.3	Head of Records Management; Information Security Manager	Further structure and content amendments

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
Information Governance Group	29/8/08	1.0
Ratified by:		
RCAG	21/10/08	1.0

Published on:	**Date**	**By**	**Dept**
The Pulse	14/10/08	Records Manager	GDU
Website	10/03/10	Records Manager	GDU

Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
	Information Security Policy	
	IM&T Change Control Procedure	

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1.0 Introduction

Laptop computers taken outside secure NHS environments are subject to additional security risks.

Laptop loss will mean not only the loss of availability of the device and its data, but may also lead to the disclosure of patient or other sensitive information. This loss of confidentiality, and potentially integrity, will often be considered more serious than the loss of the physical asset.

The impact of unauthorised access and tampering to a laptop, particularly if there are repeated opportunities for access, may extend far more widely than the laptop itself and may:

1.1 Lead to continuing (and undetected) compromise of information on the laptop itself;

1.2 Undermine security measures (including the encryption) intended to protect information on the laptop in the event of loss or theft

1.3 Lead to compromise systems to which the laptop is connected, for example, an NHS organisation's networked systems that are accessed from the laptop under an approved remote access arrangement

2.0 Objective

To ensure laptops and the information stored on them are secure whilst in use, storage and transportation.

3.0 Scope

This policy covers all laptops provided by the Trust, whether in use at the office, at home or anywhere else.

4.0 Responsibilities

4.1 The Information Governance Group will monitor this policy and any other relevant procedural documents to ensure laptop assets are appropriately managed and secured.

4.2The Information Security Manager has responsibility for reviewing this policy, keeping it up to date and reflective of current technology.

4.3 IM&T Customer Services is responsible for implementing standards and procedures in support of the Laptop Security Policy

4.4 All staff who have been allocated a laptop have a responsibility to ensure that they are kept secure and that access is restricted to their own use.

5.0 Policy

5.1 Laptop Approval

5.1.1 All Laptops issued to LAS staff must be approved by the appropriate line manager
5.1.2 Requests for Laptops by LAS staff must be lodged through the IM&T Service Desk in order to create an audit trail
5.1.3 Management approval for Laptops must be included in the IM&T Service Desk request

5.2 Laptop Asset Register

5.2.1 IM&T will asset tag all laptops for tracking purposes
5.2.2 IM&T are responsible for keeping a register of Laptop assets including who the asset has been assigned to and when
5.2.3 IM&T are responsible for periodically cross-checking the Laptop asset register to ensure the Laptop is assigned to the correct member of staff

5.3 Laptop Usage Training

5.3.1 All LAS Laptop users will receive training on how to appropriately use and secure Laptops (including remote access functionality), which may be provided in person by IM&T staff or through an information guidance sheet issued with the Laptop

5.4 Laptop Security

5.4.1 All Laptops must be physically secured at all times when not in use and IM&T will provide staff with a cable lock, keys and usage instructions on request.

5.4.2 IM&T will provide staff with a Laptop bag to protect it from damage and weather conditions

5.4.3 All Laptops will be configured by IM&T with a standard image and security baseline of defined applications and configurations.

5.4.4 IM&T will periodically perform penetration tests on Laptops to ensure configuration changes and updates have been applied in a secure manner

5.4.5 All Laptops will be configured with a working personal firewall

5.4.6 All laptops will be configured with disk level encryption which meets UK Government standards.

5.4.7 All laptops must be connected to the corporate network at least once every three months for a minimum of two hours to allow system updates to install.

5.4.8 Staff using Laptops for remote access must only do so through the authorised remote access connection method configured by IM&T as per the VPN Policy, which is under development.

5.4.9 Where large quantities of NHS data are held on a single laptop risk assessments must consider the impacts of loss of all the data. Note that deleted files should be assumed to persist on the laptop’s hard disk.

5.5 Laptop Data Storage

5.5.1 All staff who have a requirement to store personal identifiable information including patient information on their laptops must gain permission from their department head as it is LAS policy for sensitive data stored on laptops to be kept to a minimum.

5.6 Laptop Reassignment, Erasure & Disposal

5.6.1 IM&T will securely erase all information contained on laptops before they are disposed or reassigned to another member of staff.
5.6.2 IM&T will update the IM&T asset register upon asset re-assignment or disposal
5.6.3 IM&T are responsible for ensuring appropriate erasure tools and techniques are used
5.6.4 IM&T must authorise any re-configuration, re-assignment, erasure or disposal of Laptop assets

5.7 Lost/Stolen Laptops

5.7.1 Lost/Stolen Laptops must be reported immediately to the IM&T Service Desk who will immediately escalate the incident to the Information Security Manager for investigation

IMPLEMENTATION PLAN	
Intended Audience	For all staff
Dissemination	Available to all staff on the Pulse
Communications	Revised Procedure to be announced in the RIB and a link provided to the document
Training	IG training
Monitoring	IGG monitoring and audits/spot checks