London Ambulance Service NHS Trust

IM&T Remote Working Security Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This document establishes the Information Security Controls that are to be adhered to in line with remote working.

Sponsor Department: IM&T Information Security

Author/Reviewer: Information Security Manager. To be reviewed by August 2015

Document Status: Final

Amendment History			
Date	***Version**	**Author/Contributor**	**Amendment Details**
13/08/12	1.2	Director IM&T	Ratified by SMG ' with minor amendment @ page 6 – 'All staff & third parties'
16/07/12	1.1	IG Manager	Document Profile & Control update
21/02/12	0.4	IS Manager	Equality Analysis added.
23/01/12	0.3	IG Manager	Appendix 2 (LA441) amended by IGG meeting on 20/01/12
18/01/12	0.2	IG Manager	Reformatting
18/11/2011	0.1	IM&T Security Manager	Initial Draft

***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**
ADG	27/06/12	1.0
Ratified by:		
SMG	13/08/12	1.2

Published on:	**Date**	**By**	**Dept**
The Pulse	20/08/12	Governance Co-ordinator	GCT
LAS Website	20/08/12	Governance Co-ordinator	GCT
Announced on:	**Date**	**By**	**Dept**
The RIB	21/08/12	IG Manager	GCT

Equality Analysis completed on:	**By**
20/02/2012	IM&T Equality Assessment Team
Staff side reviewed on:	By

Links to Related documents or references providing additional information		
Ref. No.	Title	Version
TB/048	Information Security Policy	2.0
TB/060	Acceptable Use of Information and Communications Systems	2.0

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 Introduction

This Policy provides instructions and guidance for using devices capable of remotely working on LAS information while located at home or other external locations. This incorporates both using an LAS supplied device to work on material stored on the device, or remote network connections to LAS via remote dial-up or broadband connection. Generally the devices used for remote working will be mobile devices that are also used to connect directly to LAS wired or wireless networks when located in the Trust's premises.

The use of portable computing devices and remote access to systems is increasing within the LAS as a means of supporting flexible working and allowing staff access to information resources wherever they are working. While the use of mobile equipment and remote working enables LAS to achieve its business objectives, the security of such equipment must be maintained in order to manage and prevent unacceptable risks arising through the use of unapproved or unsafe working practices.

Remote working and the use of mobile devices requires users to adopt supplementary security practices while working remotely. The nature of devices that can be used both internally and externally exposes the LAS to additional threats that may expose LAS systems to outside threats.

This Policy has been designed in accordance with the requirements of the Information Governance Toolkit (v9) and the control statements contained in ISO27001:2005, the international standard for information security management.

This document supports the objectives of the LAS Information Security Policy (TP/048) and should be applied in conjunction with the Policy for the Acceptable Use of IT and Communications Systems (TP/060).

2 Scope

The security issues in this Policy relate to physical security of mobile devices, confidentiality of paper and electronic data, and acceptable usage instructions pertaining to users working externally.

It applies to all authorised users of LAS information including permanent and temporary staff employed within LAS, all contractors, and third parties who have legitimate access to LAS information, information assets and/or LAS ICT infrastructure.

For the purpose of this Policy, information includes data stored on mobile data devices, transmitted across networks, printed out or written on paper, sent out by

fax, stored on disk, tape and other electronic media or spoken in conversation or over the telephone.

All information that is created, processed, stored or transmitted (physically or electronically) during the course of LAS business activity is an asset of the organisation and as such is governed by this Policy.

3 Objectives

The objectives of the Trust's policy on remote access are:

3.1 To provide staff with security instructions while working remotely;

3.2 To preserve the integrity, availability and confidentiality of the Trust's information and information systems by defining security requirements associated with remote working;

3.3 To manage the serious risk of financial loss, loss of patient confidence or other business impacts which may result from a failure in security of remote services;

3.4 To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Trust is adequately protected under computer misuse legislation.

4 Responsibilities

4.1 LAS Board

The LAS Board is ultimately responsible for ensuring that remote access to LAS resources is managed securely;

4.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Officer is responsible for providing clear authorisation for all remote access users and the level of access provided;

4.3 Information Governance Group (IGG)

The Information Governance Group (IGG) will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks;

4.4 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information, this Policy supports the Caldicott function.

Information Governance Manager

Responsible for maintaining records and applying information management through liaison with other LAS functions to deliver effective Information Security.

4.5 Information Security Manager

The IM&T Information Security Manager will ensure that user profiles and logical access controls are implemented appropriately for remote access services and, through risk assessments, ensure that controls are being applied effectively;

4.6 Line Managers

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

4.7 All staff and third parties

All staff and third parties using remote access, including webmail, are responsible for complying with this Policy and associated standards. They must safeguard corporate equipment and information resources, and notify the Trust immediately of any security incidents and breaches;

Users are responsible for mobile devices and must return them to LAS when no longer needed or on termination of contract. Likewise users must notify the Service Desk if they no longer need their remote access account, so that these can be disabled.

5 Definitions

For the purposes of this policy the following definitions apply:

Mobile Computing	The use of an LAS Mobile Data Device in any location and/or the processing of LAS information away from the premises of LAS.
Teleworking	The authorised use of LAS equipment and/or personal computing resources, to carry out LAS work (or to manage staff delivering such services) from home (or from authorised third party premises), whether on a permanent or other regular basis.
Mobile Data Devices	This includes any removable media or mobile device that can store data. Typically within the LAS environment this consists of: Laptops, Smart phones, such as Blackberry, and mobile phones. But may also apply to MP3 players, digital cameras, digital audio and visual recording/playback devices and any other device that stores data.
Mobile Media	Any physical item that can store information and requires another device to access it. For

	example: CD/DVD's, tapes, floppy disc, digital storage device (flash memory cards, USB discs / memory sticks & portable hard drives).
Personal Data	Data which relates to an individual who can be identified from that data as defined in the Data Protection Act 1998.
Business Critical Information	Where the loss of data would have a significant impact on the performance, reputation or operational effectiveness of LAS. This may include but is not limited to financial, patient, staff and project tender data.
Locally saved Files and Folders	When the network is unavailable files that are stored on the local computer are called *locally saved files*. If work is carried out offline (i.e. when the network is not available) then changes will have to be updated to the LAS stored version when the network becomes available. Care is required when other users may have been working concurrently on the central LAS file.

6 Risks Associated with Remote Working

The LAS recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

6.1 Disruption or unavailability of network, systems or information resources;

6.2 Degraded performance of systems accessed via remote connections;

6.3 The potential loss or corruption of sensitive data;

6.4 The possibility of a breach of confidentiality;

6.5 The likely loss of or damage to mobile equipment;

6.6 The possibility of a breach of legislation or non-compliance with regulatory or ethical standards.

7 Mobile Device Security

7.1 Disk Encryption

7.1.1 All LAS mobile data devices must have disk encryption installed and enabled. Unauthorised removal or disabling of encryption will be considered a serious disciplinary issue.

7.1.2 Staff must inform the ICT Service Desk if they believe that their equipment is not encrypted. Staff must not continue to use knowingly unencrypted devices.

7.1.3 Any mobile media device connected to LAS mobile devices (e.g. USB memory sticks) must have approved LAS encryption enabled before any information is stored.

7.2 Physical Protection

Mobile computing devices are valuable assets and care should be taken when they are removed from LAS locations. Consider the following when moving the devices from one site to another or when using it in a non secure environment:

7.2.1 Any staff member who removes Information Assets, including paper files, from LAS premises is responsible for ensuring their safe transport and storage.

7.2.2 Never leave access control devices, such as RSA tokens, in the same bag as the mobile device.

7.2.3 Always lock devices when not in use.

7.2.4 Information assets must not be left unattended in a public place, when carrying the device between locations, keep it in view at all times. Airport lounges and public houses are prime areas where devices go missing as they are busy and people may well be distracted. Consider carrying it in an unmarked bag to avoid advertising its presence.

7.2.5 Try not to leave devices unattended in a car, but if it is absolutely necessary, lock it away in the boot making sure that no one sees this done.

7.2.6 Do not leave the devices visible on the passenger or rear seats even while driving. Valuable items can be snatched while the car is stationary at traffic lights or in a queue.

7.2.7 Try to avoid leaving a device in a hotel room whilst out unless it has a suitable safe. Most hotels have facilities to lock away valuable items at reception.

7.2.8 Memorise passwords and PIN numbers and destroy any written note as soon as possible. Never leave a note of the password or PIN with the device.

7.2.9 Do not remove any asset tag fixed to a device as this identifies the asset to the Service Desk.

7.2.10 When in transit devices must not be placed in locations where they could easily be forgotten e.g. overhead racks, taxi boots, train stations, exhibition halls etc.

7.2.11 Whenever leaving a device unattended, for even a short time, the screen saver lock must be activated to prevent unauthorised users accessing LAS data.

7.2.12 Where the device is not going to be used for a longer period of time, it must be shut down and locked away securely.

7.2.13 Equipment must be transported in a secure, clean environment.

7.2.14 Appropriate packaging should be used to prevent physical damage (laptop bags, etc).

7.2.15 Users must be aware of the fact that carrying or using a laptop computer in a public place is likely to draw attention to them and will also increase the risk of both theft and the unauthorised disclosure of information on the screen.

8 Remote Access Requirements

To lessen the potential risks of working remotely, additional mechanisms must be in place to assure the authentication, authorisation, and accounting of all users authorised to carry out work remotely. These include:

8.1 All users must be registered and authorised by their Director for remote access, Appendix 2 of this policy contains the appropriate application form (AS 441), which is also available on the Pulse.

8.2 The IM&T Systems Group is responsible for ensuring a list is kept of all remote access users.

8.3 Authentication:- User identity must be confirmed by the addition of strong, multi-factor authentication in addition to normal authentication methods.

8.4 Authorisation:- Remote users must be limited to only having appropriate remote access to the information they require when away from the office. This may differ from the data they can access when working within LAS locations.

8.5 Security monitoring, such as by intrusion detection systems, must be used to monitor network activities associated with remote working.

8.6 Data Protection

8.6.1 Staff must not remove Personal Data or Business Critical Information from site without authorisation from his/her Line Manager.

8.6.2 All staff must keep Personal Data or Business Critical information storage on portable equipment such as laptops to a minimum. When the data is no longer needed it is the user's responsibility to remove it.

8.6.3 Staff must not disable the virus protection software, disk encryption or any installed firewall software on their mobile device.

8.6.4 It is the responsibility of staff to ensure data saved on the mobile device is copied to a LAS network location as soon as possible. This is to guard against the risk of data loss if the device is lost, corrupted or broken.

8.6.5 Where LAS sensitive data or information files need to be stored on a mobile device, additional protection against unauthorised access (for example password protecting files) should be used.

8.6.6 Staff must not install unauthorised software or download software/data from the internet.

8.6.7 Staff must not dispose of any media (including paper) containing LAS information off-site. Waste must be returned to a LAS location for secure shredding or recycling.

8.6.8 All potential and actual security breaches will be investigated and, where appropriate, reported in accordance with the requirements of the LAS Serious Incident reporting procedures.

8.6.9 Accessing, saving, copying and storage of LAS sensitive data[1] or information on staff owned equipment is strictly forbidden. Staff may only use Trust supplied, encrypted machines and official LAS USB data sticks to store data.

8.6.10 Staff must not send LAS sensitive data or information to personal email addresses i.e. Users may not send LAS data to their, or another's, non-LAS email address;

[1] Sensitive data includes anything labelled NHS Confidential, NHS Protect, or identifiable patient data or sensitive financial information.

8.6.11 The confidentiality and integrity of data passing over public networks must be maintained using LAS approved encryption techniques, users must not attempt to implement unauthorised remote access to the LAS.

8.6.12 Users must immediately report lost or stolen Mobile Data Devices and/or Media to the IM&T Service Desk, or out of hours, to the IM&T On Call Duty Manager. Incidents involving mobile devices will require an incident report completed as directed by the LAS Serious Incident Policy(TP/006) and related procedures.

8.6.13 LAS will undertake regular fraud preventative exercises in order to detect unsuitable usage (for example to review frequently dialled telephone numbers, high cost calls, calls dialled outside normal working hours, calls to premium numbers or foreign countries).

8.6.14 Only officially approved, secure courier services are to be used to transport unaccompanied packages containing sensitive information. Additionally tamper proof packaging will be used.

8.7 Usage in any Public Accessible Area

8.7.1 Do not use a device in public areas e.g. on a train or at an airport, where the password, or data, can be observed as it is entered (known as shoulder surfing) or the data can be read on the screen.

8.7.2 Staff must not attempt to connect Mobile Data Devices to public Wi-Fi networks. If a user is going to a conference or hotel where this is required, a ticket should be raised with the Service Desk for consideration by the Information Security Manager.

8.8 Guests to LAS Premises with Mobile Devices

8.8.1 Visitors may be given permission to connect devices to official ‘LAS guest’ wireless networks in order to acquire internet access. Guests must agree to use these connections in accordance with the LAS Policy for the Appropriate Use of Information and Communications (TP/060) and for no other purpose.

8.9 Rules for Usage of Mobile Devices

8.9.1 Access to any form of Remote Access Device is restricted to the member of staff to whom it was issued; remember that other family members or visitors may not understand the need for information security. LAS equipment should be locked away when not being used.

8.9.2 SIM cards must not be transferred between different mobile devices; such as laptops, Blackberries, mobile phones etc, as different tariffs may apply.

Should there be a requirement to change the device with which the SIM card is associated, a Change Request should be submitted via the Service Desk.

8.9.3 Any portable device that is owned by LAS, which has internet connectivity, must be used in accordance with the LAS IM&T Acceptable Use of IT and Communications Equipment Policy. Particular attention should be paid to the provisions relating to access to unsuitable material and activities which may compromise network security. This applies wherever the equipment is used.

8.9.4 LAS is responsible for the safety testing of supplied equipment and the annual electrical safety Portable Appliance Testing (PAT). Staff who use mobile devices are responsible for ensuring that these checks are undertaken.

8.10 Staff-owned Equipment

8.10.1 The use and storage of Personal Data or Business Critical Information on staff owned equipment is strictly forbidden. Staff may only use LAS supplied equipment for this purpose.

8.10.2 To prevent viruses, and related security risks, users are not allowed to connect their own personal equipment to LAS networks unless express permission has been granted by the IM&T Director.

8.10.3 The use of personally-owned phones is prohibited for business use with regard to data transfer and storage. Staff must not synchronise their personal phone devices (including iPhones, Smartphones and Blackberry's) with their business Outlook information, since doing so will result in an unencrypted copy of potentially personal identifiable data being stored on the device.

8.10.4 Voice calls from a personal phone for business purposes are permitted.

8.10.5 Staff may only use non NHS owned equipment for work related activities where no information is stored on the device.

9 Teleworking – (Working from Home)

The following statements apply to Teleworkers, working from their home environment:

9.1 Staff must ensure the security of information and mobile devices within their home from theft. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it, should be neatly stored away, out of site of ground floor windows and doors.

9.2 Any staff members defined as Teleworkers are responsible for ensuring that their work conditions at home comply with health and safety regulations and LAS policies and procedures. Staff must undertake a display screen equipment

risk assessment as detailed in the Display Screen Equipment Policy (DSE) and a copy of this assessment must be retained on their personnel file.

10 Audit of Teleworking

10.1 LAS reserve the right to undertake regular audits of remote/teleworking arrangements to ensure that all users are approved, assets can be accounted for, that secure remote access is used, and any confidential/sensitive information is securely transported or stored in a remote location.

IMPLEMENTATION PLAN	
Intended Audience	All staff with, or applying for remote working devices
Dissemination	The Pulse and the LAS Website
Communications	No specific communication
Training	No
Monitoring	Remote working procedures are an essential part of securing LAS information from data leakage. Security incidents and subsequent investigations will be reported and considered via the Information Governance Group. Compliance will be measured in terms of the number of breaches and the behaviour of users working remotely. All results will be presented to the **Information Governance Group** at least annually. The IGG will report annually to the RCAG meeting, including any changes in policy and procedure in reaction to experience of actual LAS related events.

Appendix 1

Information Governance Toolkit Compliance Statement

The LAS are required to provide an appropriate level of information governance based upon the requirements of the Information Governance Toolkit (IGT). This Policy supports the following requirements of the Information Governance Toolkit v9:

Requirement 201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users
Requirement 314	Policy and procedures ensure that mobile computing and teleworking are secure

Appendix 2

Application for Remote Access Account Form LA441

Please complete and send this form to: **IM&T Service Desk**.

This form should be completed by staff requiring remote access to conduct LAS work. Please note all details, including approval by both a Director and the Senior Information Risk Owner (SIRO), must be completed before sending to the Service Desk.

1) Staff Details

Full Name: …….. Title: …….....

Job Title: ……..… Department: ……..

Contact Number: …… Email: .....…….....

2) Staff Agreement to Conditions of Acceptance

I have read the conditions specified in the Remote Working Security Policy and the LAS Acceptable Use of IT and Communications Policy and agree to abide by these while using a mobile device or teleworking.

I undertake to return mobile devices to IM&T if requested or when I no longer require them. I acknowledge I am not authorised to transfer devices to another LAS employee for use, and that IM&T may periodically require access to the device.

I undertake to connect LAS laptops, and devices that require routine updates, to the LAS LAN at least once every 6 weeks, and for a period of 2 hours, so that automatic updates can occur.

I accept that upon leaving LAS employment, all laptops, accessories and bags will be returned to IM&T.

If the laptop issued to me is damaged or lost I will immediately report this via the IM&T Service Desk, or out of hours, to the IM&T Duty Manager, and complete the incident forms as described in the Serious Incident Policy (TP/006).

Signed: …….…….. Date: ……..

3) To be completed by the Applicant's Director

In approving this application, I accept cost of providing remote access facilities and have considered the additional risks of sensitive information leakage and equipment loss.

Signed: …….Director) Print Name: ……..…….……

Date: ……/……/……..

4) To be completed by the Senior Information Risk Owner (SIRO – Director of IM&T)

I approve the granting of remote computing facilities for the above names individual.

Signed: ……..SIRO) Print Name: ……..…….……

Date: ……/……/……..

Once countersigned by a Director and the SIRO, please forward this form to the IM&T Service Desk.