London Ambulance Service NHS Trust

Policy for the Acceptable Use of IT and Communications Systems

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This policy relates to the use and monitoring of LAS IT and communications systems, including telephones, mobile telephones, facsimile machines, computers (including laptops and personal organisers), email, the internet, the intranet and extranet.

Sponsor Department: IM&T Information Security

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

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
28/05/12	2.1	IG Manager	Doc Profile & Control update
21/02/12	1.3	IS Manager	Addition of S.10.12 & Equality Analysis
18/01/12	1.2	IG Manager	Reformatting
04/01/2012	1.1	Information Security Manager	Review and inclusion of Internet and Email Policies
07/07/2010	0.8	Information Security Manager	Minor Amendments, updated additional comments
06/07/2010	0.7	Head of Records	Amendments
02/07/2010	0.6	Records Manager	Re-format
23/06/2010	0.5	Senior Information Risk Owner	Comments on breach of policy section
29/01/2010	0.5	Information Security Project Manager	Updated definitions section
03/11/2009	0.4	Information Security Manager	Restructure of content and minor additions
21/10/2009	0.3	Information Security Project Manager	Updated inputs from IM&T managers
13/10/2009	0.2	Information Security Manager	comments
13/10/2009	0.1	Information Security Project 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	27/03/12	2.0
SMG	14/07/10	1.0
Ratified by (If appropriate):	**Date Approved**	

Published on:	Date	By	Dept
The Pulse (v.2)	28/05/12	IG Manager	G&C
LAS Website (v.2)	28/05/12	IG Manager	G&C
The Pulse (v.1)	27/07/10	Records Manager	GCT
LAS Website (v.1)	27/07/10	Records Manager	GCT
Announced on:	**Date**	**By**	**Dept**
The RIB	29/05/12	IG Manager	G&C
The RIB	03/08/10	Records Manager	GCT

Equality Analysis completed on:	By
17/02/2012	IM&T Equality Assessment Team
05/07/10	Head of MI, Information Security Manager, and Head of Records Management
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	Title	Version
	Information Security Technology Techniques – Information Security Management System Requirements 27001: 2005 – British Standards Organisation	
	Regulations of Investigatory Powers Act, 2000 http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000023_en_2	

	Computer Misuse Act, 1990	
	Data Protection Act, 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1	
	Freedom of Information Act 2000	
TP/012	Data Protection Policy	
TP/022	Freedom of Information Policy	

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 supports the Information Security Policy (TP/048) and relates to the appropriate usage, and monitoring of, the London Ambulance Service NHS Trust (LAS) IT and Communications systems, including telephones, mobile telephones, facsimile machines, computer devices (including workstations, laptops and personal organisers), email, the internet, the intranet and extranet.

The Trust provides the IT and communication systems for business purposes and the use of these systems at all times is subject to this Policy.

Effective security is a team effort involving the participation and support of every LAS employee and authorised users who deals with information and/or information systems.

It is the responsibility of every user to read and understand these requirements, and to conduct their activities accordingly.

2 Scope

This Policy applies to all LAS employees, contractors and partners who use the Trust's IT and communication systems.

3 Objectives

This Policy is to ensure that all staff are aware of their responsibility to use Trust IT and communication systems and to raise awareness to staff that security of Trust resources and information is everyone's responsibility.

4 Responsibilities

Director of IM&T

The Director of IM&T is also the Senior Risk Owner (SIRO) and is accountable to the Trust Board for Information Security and responsible for reporting Information Security risks to the Risk, Compliance and Assurance Group.

Caldicott Guardian

Responsible for protecting the confidentiality of patient and service-user information and 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.

Information Security Manager

Responsible for maintaining and reviewing information processing systems against information security controls and maintaining Information Security

Management System (ISMS) pertaining to technical policies, standards and guidelines.

Information Governance Group (IGG)

Chaired by the Director of IM&T this Group will monitor the implementation of this policy.

Information Asset Owners (IAO)

Information asset owners are the custodians of identified business information. Their role is to understand what information is held, what is added and what is removed, how personal information is moved, and who has access and why. IAO are required to understand and address risks to the information, and ensure that information is fully used within the relevant laws, and provide written input to the SIRO on the security and use of the assets they are responsible for.

Line Managers

Responsible for ensuring staff work in line with the Information Security Policy and other published security policies and controls.

All staff and third parties

Responsible for ensuring information security is appropriately considered and that the Information Security Policy and these key controls are adhered to.

5 Definitions

For the purposes of this policy the following definitions apply:

Confidential	Material containing person identifiable information or marked “confidential”. For example; patient notes, staff records, referrals, etc
Data	Information which is: being processed by means of equipment operating automatically in response to instructions given for that purpose recorded with the intention that it should be processed by means of such equipment recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system does not fall within paragraph a), b) or c) but forms part of an accessible record as defined by section 68 (see Accessible Record) *[DPA,1998]*
Data subject	An individual who is the subject of personal data *[DPA,1998]*

Information Commissioner	A person appointed by Government to administer the provisions of the Data Protection Act and Freedom of Information Act. Before the FOIA, 2000, called the Data Protection Registrar (1984) or the Data Protection Commissioner (1998)
Password	Confidential authentication information composed of a string of characters
Patient information / Personal information / Personal data	see “person identifiable information”
Person identifiable information	Data which relate to a living individual who can be identified: from that data and other information in the possession of, or likely to come in the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual *[DPA,1998]*
Processing (in relation to data)	Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: organisation, adaptation or alteration of the information or data retrieval, consultation or use of the information or data disclosure of the information or data by transmission, dissemination or otherwise making available alignment, combination, blocking, erasure or destruction of the information or data *[DPA,1998]*
User	Any individual employees, contractors and agents (“staff”) who use the Trust’s IT and communication systems.
Blogging	The act of posting information on a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or

	video. Entries are commonly displayed in reverse chronological order as a form of diary.

6 Acceptable Use of IT and Communication Systems Policy

Breach of this policy in regards to the use of the Trust's IT and communication systems will be considered a serious disciplinary matter and will be dealt with in line with the Trust's disciplinary process. Examples of offences which may be considered to be misconduct or gross misconduct include: (This list is not exhaustive)

6.1 The unauthorised removal, copying or distribution of sensitive LAS information, including patient records, financial data or reports;

6.2 Introducing a virus to the computer system by inserting a USB memory device, CD or DVD into a Trust computer without running a virus check, via email or from downloading a file from the Internet;

6.3 Misuse of the computer system which results in any claim being made against the Trust;

6.4 The connection of an unauthorised device to the network;

6.5 Use of the internet for criminal activity;

6.6 Excessive visiting of non job related internet sites during the normal working day;

6.7 Accessing pornography or any other illegal material on the internet and/or circulating it;

6.8 Sending abusive e-mails or other communication;

6.9 Unauthorised copying or modifying of copyright material;

6.10 The unauthorised copying of LAS source code, software or data files.

7 Personal Use and Ownership

While LAS wishes to provide a reasonable level of personal privacy, users must be aware that the data they create on LAS ICT systems remains LAS property. Due to the need to protect LAS information resources, the LAS cannot guarantee the privacy of personal information on any device used for LAS business.

For security and network maintenance purposes, designated authorised individuals, within the LAS, may monitor equipment, systems and network traffic at any time.

Personally purchased equipment, such as PDA's, mobile phones or music players may never be attached to LAS ICT equipment or networks. The LAS reserves the right to inspect any device brought within its premises or connected to its networks.

8 Passwords

Passwords play a significant role in maintaining security of LAS systems. Attackers may try to break passwords in various ways. Generally the longer the password, the more difficult it is to be broken, but other attacks may rely on the likelihood that a user has selected a weak password. A weak password may be one or more words (in English or any other language), perhaps with numbers added or replacing letters (e.g. 'O' for 'o'), or where a piece of personal information, such as a pets name has been used. Alternatively, attackers may rely on users writing down passwords or allowing themselves to be overlooked when typing in the password.

Each User must be aware that all activity undertaken using their account will be attributable to them individually.

8.1 Generic Password Policy

The following rules apply to all users and all systems:

- Users must never divulge passwords to anyone. The Service Desk or System Administrators do not need to know users' passwords;
- If a user's password has been divulged in any way it must be changed immediately and an incident raised with the Service Desk;
- If a user needs to write down a password, it must be secured in an envelope that has been signed and the seals taped. The envelope must be stored in a lockable container that is appropriate for the sensitivity of the system;
- Users must not reuse a password on any other system-each password must be unique;
- When logging on to a system or unlocking the device, users must ensure that they are not being overlooked when typing the password on the keyboard.

8.2 Password Creation

Each LAS system will have rules covering the strength of password required, this will include: the minimum password length, how often the password needs to be changed, the policy for password reuse; and instructions how to avoid choosing weak passwords.

9 E-mail

Users are required to comply with the following rules for email usage:

9.1 Email correspondence is not private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. Users must take into account the fact that any email they send may be read by a person other than the intended recipient.

9.2 Email attachments must not be downloaded to a non LAS computer while accessing the Trust's network remotely.

9.3 Sensitive or confidential information, especially relating to patients personal identifiable information must be not be sent externally to any non London Ambulance email address, N.B. The Connecting for Health, NHSmail service is appropriate for this type of communication.

9.4 Auto forwarding of the Trust emails to personal email accounts is prohibited.

9.5 All messages and files are automatically scanned for viruses before being introduced into the network, but this does not provide a complete guarantee of protection. All employees have an obligation to be cautious when opening emails and attachments to emails from unknown sources. If a user has any doubts about opening an email or attachment, they should contact the IM&T Service Desk.

9.6 Contracts can be entered into by e-mail in the same way as they are by letter or on the telephone. Users must, at all times, take care to ensure that they do not inadvertently enter into contracts which bind the Trust by email, and they should be aware that contracts must only be entered into in accordance with the normal procedures.

9.7 Users must not, under any circumstances, send messages or attachments whether within the Trust or outside the Trust which reasonably could be considered to be:

- Abusive including the use of foul language;
- Malicious;
- Discriminatory in any sense (e.g. sexual orientation, age, race, religion, gender or disability);
- Defamatory about any other person or organisation;
- Bullying or intimidating in content;
- Containing sensitive or confidential LAS information without the appropriate security measures in place.

9.8 If a user receives any such messages from outside the Trust, they must delete them and not forward them either within or outside of the Trust. If the email causes a user distress, they should seek support from their manager.

9.9 The use of web based email must not be used for transferring files to or from LAS.

10 Internet

Users are required to comply with the following requirements:

10.1 Internet access is supplied for official LAS business. Staff are authorised to access the internet for limited personal business but this should be reasonable and not adversely impact on that member of staff's job.

10.2 The Trust has put technical measures in place to prevent access to Internet web sites which contain explicit, illegal or other inappropriate materials. If a user needs to access a site which contains such materials for the purposes of their role, they can request access through the IM&T Service Desk.

10.3 Unless expressly authorised to do so, staff are prohibited from sending, transmitting, or otherwise distributing the Trust's information or data to external third parties.

10.4 Production, accessing, downloading, dissemination or storing of non-business related solicitations (e.g. mass emails), destructive code (e.g. viruses), pornographic text or images, fraudulent or defamatory images or text or anything that may be construed as unlawful, harassing or offensive to others is prohibited. This list should not be regarded as exhaustive.

10.5 Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages and other material.

10.6 No software may be downloaded or executed from the internet by staff under any circumstances, unless authorised by the Director of IM&T.

10.7 Instant messaging or other chat type communication is prohibited.

10.8 Use of web based email systems must not be used for sending or receiving attachments.

10.9 Video and audio streaming (e.g. online radio) is prohibited unless authorised by the Director of IM&T.

10.10 By-passing the Service's network to access the Internet by modem or other means is prohibited unless the computer is not connected to the Trust's network.

10.11 Staff and contractors using blogging sites, such as Twitter, must not refer to LAS activities unless authorised by a Director.

10.12 Staff should carefully consider the appropriateness of comments they make via social networking websites such as Facebook, My Space and LinkedIn. Unauthorised comments on LAS activities is discouraged and instances where the Trust is brought into disrepute may constitute misconduct or gross misconduct and disciplinary action applied.

11 Avoiding Malware through Responsible Usage

All LAS systems must have some form of anti-virus software installed. If a user has any doubt about the anti-virus software on a system, or are unsure if it is working, they must contact the Service Desk.

The following represents basic usage requirements to reduce LAS exposure to malware:

11.1 Emails are a common source of malware. If a user receives unsolicited email with attachments, they must not open them, but instead delete them or contact the Service Desk. Users must not forward the email to anyone, including the Service Desk;

11.2 Emails that contain warnings of viruses circulating on the Internet are a nuisance and almost always inaccurate. Do not forward virus warnings unless authorised;

11.3 Web links in e-mails are a common source of malware/unauthorised programs. Should a user wish to access the site, they should enter the relevant URL into the browser window as opposed to clicking on the link in the email;

11.4 Dialog boxes are used to confirm actions with the user, such as confirming the user wishes to install a program. Users must never blindly accept these and always cancel unexpected dialogue boxes;

11.5 Removable Media - malware can spread from system to system on removable media. Users can help by:

- Following any specified usage guidance for removable media and check it for viruses and other malicious code after inserting it into a PC/Laptop or other ICT device.
- Incident Reporting- If malware has entered LAS systems, the impact can be reduced if the correct authorities know about it early. Users can help, even if they have made a mistake, by letting us know, incidents can be contained before serious damage is done.
- Report to the Service Desk any unusual or suspicious activity or events such as suspected or actual compromise of LAS information, LAS information assets or LAS ICT infrastructure.

12 Maintaining Confidentiality of LAS Information

12.1 Users must not use the Trust's IT and communications systems whether alone or in conjunction with any other device to make any unauthorised disclosure or copy of confidential information belonging to the Trust.

12.2 Transportation of electronic Trust data must only be via LAS authorised encrypted media.

12.3 The unauthorised disclosure or copying of information belonging to the Trust is likely to be treated as a disciplinary offence and could give rise to dismissal for gross misconduct.

12.4 Such confidential Information may include, without limitation details of:

12.4.1 Business contacts, associates, lists of suppliers and details of contacts with them;

12.4.2 Identities of patients and/or staff;

12.4.3 Expenditure levels and buying and Trust specific pricing policies;

12.4.4 Proposals plans or specifications for the development of existing services and of new services;

12.4.5 Details of the employees and officers of the Trust and of the remuneration and other benefits paid to them;

12.4.6 Presentations, tenders, projects, joint ventures, mergers and developments contemplated, offered or undertaken by the Trust;

12.5 Employees are prohibited from revealing any LAS confidential or proprietary information, trade secrets or any other company or patient confidential material when engaged in blogging;

12.6 Notwithstanding the above, the Trust will comply with the Freedom of Information Act, 2000 and the Data Protection Act, 1998 and will deal with any such requests in accordance with this and other legislation.

13 Monitoring and Data Protection

13.1 In order to protect the interests of the Trust and to maintain the effectiveness, integrity and security of the Trust's network, the Trust has tools in place to monitor telephone, email communication and internet use by staff.

13.2 Monitoring is undertaken using the following automatic procedures:

13.2.1 Automatic checking of emails and attachments for viruses;

13.2.2 Automatic checking of emails for multimedia attachments and offensive words;

13.2.3 Automatic checking of disks, CDs and internet sites for viruses;

13.2.4 Automatic measures in place to prevent software from being downloaded to, installed on, or deleted from the Trust's computers;

13.2.5 Automatic blocking or recording access to certain files and pages on the internet;

13.2.6 Automatic recording of telephone and mobile telephone call destination numbers;

13.2.7 Recording details of unauthorised devices attached to LAS systems;

13.2.8 Automatic blocking of access to premium rate telephone lines.

13.3 Monitoring of the content of emails, internet use or telephone calls is not routinely carried out but may be carried out for some specific security related situations. For example (this is not an exhaustive list):

13.3.1 Where the Trust has reasonable grounds to believe a staff member is breaching this or any other Trust policy;

13.3.2 Where another party may have compromised a users account to gain access to LAS systems;

13.3.3 Where there is a suspected breach of contract;

13.3.4 For the purpose of assisting in the investigation of illegal acts;

13.3.5 To comply with any legal obligations;

13.3.6 For the purpose of defending or prosecuting any legal action brought against the Trust.

13.3.7 Any monitoring deemed necessary will be undertaken in compliance with the Regulation of Investigatory Powers Act, 2000.

13.4 Users should not expect that their personal use of the Trust's IT and communication systems will remain private.

13.5 The holding, processing and disclosure of personal data is regulated by the provisions in the Data Protection Act, 1998. Personal information relating to a living individual who can be identified from that information should not be transferred unless proper checks have been made to ensure that this will not involve any breach of legislation.

Users must also comply with the Trust's Data Protection Policy (TP/012).

14 Security Responsibilities of Users

14.1 Employee access to the Trust's IT and communication systems is subject to satisfactory security checks being carried out at the reasonable discretion of the Trust.

14.2 Users provided with a portable computer, mobile phone, personal organiser and/or any related or similar equipment, must ensure its security at all times. In particular, they must:

- Never leave computer equipment including discs, CDs and DVDs in an unattended vehicle, or unattended in public;
- Keep passwords confidential. The Trust IT systems have policies in place that will force users to change them regularly;
- In order to prevent unauthorised users, lock the terminal if leaving a device unattended so that it cannot be used without entering a valid log-on ID.

14.3 If a LAS device is lost or stolen there is a serious risk of data loss. It must immediately be reported to the police, the IM&T Service Desk and the responsible user's line manager. Out of hours, the IM&T Duty Manager must be contacted.

14.4 Estates should be notified if office furniture or entry points have been damaged. The incident will be fully investigated and may be treated as a disciplinary issue if the user has failed to take adequate steps to safeguarding the security of equipment in their possession.

14.5 Users must not attempt to gain access to any part of the network to which they are not permitted access.

14.5.1 Users must take care when transferring data on USB memory devices, other files may have been inadvertently been left on the disk.

15 Equipment not provided by the Trust

15.1 Staff must not connect or attempt to connect any non-service issued device to the network without express authority from the Information Security Department. Users should be aware that the Trust has in place automatic measures to prevent and audit this.

15.2 Users must not attempt to connect any of the following devices to the Trust's network:

- An unauthorised file or information storage device;
- A mobile phone or PDA not issued by the Trust;
- An MP3 Player or similar device;

- A Laptop or any removable device not issued by the Trust;
- A gaming device;
- A camera or flash memory card not issued by the Trust.

16 Personal Use

16.1 A limited amount of personal use of the Trust's systems is permitted subject to the following conditions:

16.1.1 Work on the Trust's business must always take priority over personal usage of the Trust's systems;

16.1.2 Any personal use must not delay or interfere with the proper performance of the duties of any member of staff;

16.1.3 All outgoing emails are appended with a disclaimer clause approved by Legal Services;

16.1.4 Where a user is in receipt of personal emails they should advise the sender that these may be monitored by their employers systems;

16.1.5 Personal emails should not be stored on LAS devices and must be deleted as soon as is practical to do so;

16.1.6 Users may not use the Trust's systems to transfer, store or download information and files for their personal use including (but not limited to) music and video files and other similar formats.

16.2 If a users personal use exceeds an acceptable level in the reasonable opinion of the Trust or they do not comply with these rules, their access to the system may be curtailed and they may be subject to disciplinary action.

IMPLEMENTATION PLAN	
Intended Audience	All staff and external
Dissemination	The Pulse and the LAS Website
Communications	Revised Policy and Procedure to be announced in the RIB and a link provided to the document.
Training	Training will be provided to relevant staff via induction and other employee awareness programs
Monitoring	Information Security Manager will monitor compliance through recording security breaches and serious incidents. The Information Governance Group is already the forum for reporting and measuring compliance. An annual Group meeting will be used to discuss compliance and appropriate actions for performance improvement e.g. change training content in light of experience. The IGG will report and present recommendations through RCAG

Appendix 1

Information Governance Toolkit Compliance Statement

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 302	There are documented information security incident / event reporting and management procedures that are accessible to all staff
Requirement 313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely
Requirement 323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures