London Ambulance Service NHS

NHS Trust

Information Security Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This policy aims to state the Trust's information security posture in order to create a secure environment that will lead to high levels of confidence in information.

.

Sponsor Department: IM&T Information Security

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

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
12/03/09	1.1	Records Manager	Minor – reformatted document
20/12/08	0.4	Information Security Manager	Minor -incorporated IGG minor changes
29/08/08	0.3	Information Security Manager	Minor - Objectives revised to incorporate IGG recommendations
12/08/08	0.2	Information Security Manager	Minor - Reformat and encryption additions
11/07/08	0.1	Information Security Manager	Minor - 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**
IGG	03/02/09	1.0
Ratified by:		
RCAG	16/02/09	1.0

Published on:	**Date**	**By**	**Dept**
The Pulse	12/03/09	Records Manager	GDU
LAS Website	12/03/09	Records Manager	GDU

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
	The Data Protection Act, 1998	
	The Data Protection (Processing of Sensitive Personal Data) Order, 2000	
	The Copyright, Designs and Patents Act, 1988	
	The Computer Misuse Act, 1990	
	The Health and Safety at Work Act, 1974	
	Human Rights Act, 1998	
	Regulation of Investigatory Powers Act, 2000	
	Freedom of Information Act, 2000	
	Health & Social Care Act, 2001	
	Principles of Information Security - NHS Connecting for Health (http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security)	
	Information Security Technology Techniques – Information Security Management System Requirements 27001: 2005 – British Standards Organisation	
	Risk Management 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

The London Ambulance Service NHS Trust (LAS) is committed to creating and maintaining a secure environment for its paper based and electronic information.
The Trust firmly believes that information is crucial to success and that the secure availability of accurate information is a key goal to improved decision making.
It recognises the importance of information to the Service and its ability to function.
It recognises that patient & public confidence could be affected unless security industry good practices are implemented.

In order to maintain a secure environment, it is Policy for the Trust to follow ISO27001 (part of the BS 27000 family of standards) and in doing so have developed a set procedures as our Key Controls framework. The ISO27001 standard includes a recommendation to define an Information Security Management System (ISMS) to ensure that the Trust has key controls in place to manage information security effectively.

The impacts and costs of not protecting information can be high from a regulatory compliance, monetary and reputational perspective. The LAS is not only obligated to its patients and staff but also to those of other NHS organisations and their patients.

2. Scope

This Policy covers all Trust paper based and electronic information and information related physical assets and environments.

3. Objectives

To ensure the confidentiality, integrity and availability of paper based and electronic information and supporting processes and systems through:

1. ensuring management of physical, environmental, paper based and electronic assets meets compliance requirements of the Information Governance Toolkit.

2. ensuring all Trust staff are aware of confidentiality and acceptable use requirements through awareness campaigns and training.

3. ensuring effective controls are in place for information technology systems

4. ensuring access to physical and logical Trust assets is appropriately authorised, implemented and reviewed

5. ensuring software and applications which are developed within the Trust are done so with appropriate security controls in place

6. ensuring incidents are appropriately identified, managed and reported

7. ensuring core operational service continuity and recovery processes are in place and regularly reviewed and tested

4. Policy

4.1 Responsibilities

- Director of IM&T:

  Accountable to the Trust Board for Information Security and responsible for reporting Information Security risks to the Risk, Compliance and Assurance Group.

- Medical Director:

  Acts as the Trust's Caldicott Guardian with responsibility for patient confidentiality.

- Information Security Manager:

  Responsible for managing Information Security within the Trust.

- Head of Records Management and Business Continuity:

  Responsible for records and information management and liaising with the Information Security Manager in the delivery of effective Information Security.

- Line Managers:

  Responsible for ensuring staff work in line with this Policy and associated Key Controls.

- All staff and third parties:

  Responsible for ensuring information security is appropriately considered and that this Policy is adhered to.

4.2 Legislation

The Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of The Trust who may be held personally accountable for any breaches of information security for which they may be held responsible. The Trust shall comply with legislation listed in the Reference section of this Policy and other legislation as appropriate.

4.3 Information Security Management System

An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems. BSI published a code of practice for these systems, which has now been adopted internationally as ISO/IEC 27001:2005.

The Trust's Information Security Management System (ISMS) is made up of a number of management programmes aligned to the British Standard 27000 (BS 27000) family of standards for information security management which recommends having a Risk Management Framework specific to assessing risks to information systems and facilities. Within the Trust, this will be managed under the Risk Management Policy. The ISMS programmes are used to manage and track the implementation of the Policies and Procedures associated with each of the Key Controls listed in section seven of this document.

4.4 Key Control Framework

The Key Control framework is made up of ten information security statements which form the basis of this Policy. Each statement domain contains a number of individual control requirements specific to The Trust. These controls must be implemented in order to adhere to the security statements below. A separate Key Controls document will be maintained by the Information Security Department in order to detail specific control Polices and Procedures. The ten statements that constitute the framework are summarised below.

4.4.1 Security Policy & Organisation

The Trust will implement and maintain an information security Policy for all paper based and electronic information, supporting processes and systems. The information security Policy will be regularly reviewed by the Information Governance Group. An information security organisation framework will be implemented made up of specialist security roles in order to initiate and control the implementation of information security within the organisation.

Refer to Key Control 1 for supporting Policies and Procedural controls

4.4.2 Asset Management

The Trust will implement and maintain asset registers for paper based and electronic information. This includes asset ownership, classification, people and physical, software and communication and technology devices.

Refer to Key Control 2 for supporting Policies and Procedural controls

4.4.3 Human Resources Security

The Trust will implement appropriate controls to ensure commencing, current or exiting full-time or temporary staff and third parties are legally bound to preserve confidentiality, understand their security responsibilities and are suitable for the roles they have been asked to perform.

Refer to Key Control 3 for supporting Policies and Procedural controls

4.4.4 Physical and Environmental Security

The Trust will implement physical and environmental controls to ensure assets and facilities are appropriately protected from unauthorised access, interference, intentional damage or natural disasters.

Refer to Key Control 4 for supporting Policies and Procedural controls

4.4.5 Communications and Operations Management

The Trust will implement appropriate controls to ensure secure and controlled operational running of information management and technology assets and processing facilities.

Refer to Key Control 5 for supporting Policies and Procedural controls

4.4.6 Access Control

The Trust will implement appropriate controls to ensure physical and logical access to paper based and electronic information, physical assets, information processing facilities, business processes and core operating functions is authorised to the least amount of access required by staff to perform their roles.

Refer to Key Control 6 for supporting Policies and Procedural controls

4.4.7 Information Systems, Acquisitions and Development

The Trust will implement appropriate controls to ensure newly acquired or developed system and application designs identify security requirements prior to production release and are implemented in a controlled and secure manner.

Refer to Key Control 7 for supporting Policies and Procedural controls

4.4.8 Incident Management

The Trust will implement appropriate controls to ensure information security incidents are detected, reported, responded to and resolved within an acceptable timeframe and that incident types and reporting and escalation Procedures are communicated to staff.

Refer to Key Control 8 for supporting Policies and Procedural controls

4.4.9 Business Continuity Management

The Trust will implement management processes to ensure the timely resumption of services to the public in the event of unforeseen service outages.

Refer to Key Control 9 for supporting Policies and Procedural controls

4.4.10 Compliance

The Trust will implement appropriate controls to ensure breaches of any statutory, regulatory or contractual law does not occur and expert legal counsel will be contacted to advise on legal compliance matters.

Refer to Key Control 10 for supporting Policies and Procedural controls

4.5 Policy Exceptions

Any exceptions to this policy must be formally requested to the Information Security Manager for consideration.

IMPLEMENTATION PLAN	
Intended Audience	For all staff
Dissemination	Available to all staff on the Pulse
Communications	Revised Policy and Key Controls to be announced in the RIB and a link provided to the document
Training	IG awareness to all staff Use of encryption – methods and suitability
Monitoring	Scheduled audits of information flow – internally and externally. Annual self-assessment through the Information Governance Toolkit.

Appendix 1

Definitions

Asset

Anything that has value to the organisation

Availability

The property of being accessible and usable upon demand by an authorised entity

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes

Information Security

Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Information Security Incident

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information Security Management System (ISMS)

That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Integrity

The property of safeguarding the accuracy and completeness of assets