London Ambulance Service NHS Trust

# Information Security Policy

London Ambulance Service NHS Trust

**DOCUMENT PROFILE and CONTROL.**

**Purpose of the document**: This document establishes the Information Security Key Controls that are to be adhered to in line with the Information Security Policy.

**Sponsor Department:** IM&T Information Security

**Author/Reviewer:** Information Security Manager. To be reviewed by September 2017.

**Document Status:** Final

| **Amendment History** | | | |
|---|---|---|---|
| Date | *Version | Author/Contributor | Amendment Details |
| 10/11/14 | 3.1 | IG Manager | Document Profile and Control update |
| 16/09/14 | 2.4 | IG Manager | Addition of reference following IGG approval and Document Profile and Control update. |
| 15/07/14 | 2.3 | IS Manager | Updated section 4 and introduced new paragraphs in section 5. |
| 25/03/13 | 2.2 | IG Manager | Addition of Implementation Plan |
| 28/05/12 | 2.1 | IG Manager | Doc Profile & Control update |
| 21/12/11 | 1.5 | IS Manager & IG Manager | Further revisions following IGG. |
| 16/12/11 | 1.4 | IS Manager & IG Manager | Further revisions |
| 26/10/11 | 1.3 | IM&T Security Dept | Revised in line with new policy framework |
| 28/05/11 | 1.2 | IM&T Security Dept | Added review comments |
| 25/02/11 | 1.1 | IM&T Security Dept | Renamed document, formatted document, revised content and removed duplication, Incorporated IGG minor changes |
| 05/02/09 | 1 | IM&T Security Dept | Minor IGG changes |
| 21/12/08 | 0.3 | IM&T Security Dept | Minor IGG changes |
| 19/12/08 | 0.2 | IM&T Security Dept | Incorporated IGG minor changes |
| 11/07/08 | 0.1 | IM&T Security Dept | Initial Draft |

| For Approval By: | Date Approved | Version |
|---|---|---|
| SMT | 24/09/14 | 3.0 |
| ADG | 27/03/2012 | 2.0 |
| IM&T SMG<br>Information Governance Group | 03/02/2009 | 1.0 |

| Published on: | Date | By | Dept |
|---|---|---|---|
| The Pulse | 10/11/14 (v3.1) | Governance Administrator | G&A |
| The Pulse | 25/03/13 (v.2.2) | Governance Co-ordinator | G&C |
| LAS Website | 10/11/14 (v3.1) | Governance Administrator | G&A |
| LAS Website | 25/03/13 (v.2.2) | Governance Co-ordinator | G&C |
| The Pulse | 12/03/09 (v.1) | Records Manager | GDU |
| LAS Website | 12/03/09 (v.1) | Records Manager | GDU |
| **Announced on:** | **Date** | **By** | **Dept** |
| The RIB | 11/11/14 | IG Manager | G&A |
| The RIB | 29/05/12 | IG Manager | G&C |

| Equality Analysis completed on | By |
|---|---|
| 20/12/2011 | RL, MT, BT, GF |
| **Staffside reviewed on** | **By** |
| | |

| Documents or references providing additional information | | |
|---|---|---|
| **Ref. No.** | **Title** | **Version** |
| TP080 | Social Media Policy | |
| | Security Controls Procedural Manual | 1.0 |
| | 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 | |

**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 (LAS) is committed to using information responsibly, legally and securely to protect patients, staff and the NHS from information security issues.

The LAS relies upon information and the systems that store, process and transport it in all its operations, the sensitive nature of its operations requires that information systems are protected in terms of confidentiality, integrity and availability. LAS is trusted to handle personal information, as defined by the Data Protection Act (DPA), as well as other commercially sensitive data. The protection of this data is key, not only to ensure compliance with our legal, regulatory and contractual requirements, but also to maintain the reputation of the LAS with patients, partners, staff, the NHS, stakeholders and the general public.

This document is part of a framework of security policies, standards and guides that establish effective controls to ensure the security of information within the Trust, and demonstrates a clear commitment to information security.

This document contains high level security statements, not detailed technical controls. Additional LAS policies and guidance contain more specific advice on how to meet the requirements of this Policy.

## 2 Scope

This policy covers information security for the LAS.

It applies to all authorised users of LAS information including permanent and temporary staff employed within the LAS, all contractors, suppliers and third parties who have legitimate access to LAS information, information systems and infrastructure.

The controls set out in this Policy apply to all Trust users, information, information systems, networks and applications and those supplied under contract to it.

## 3 Objectives

The purpose of this policy and other supporting security policies is to:

- Convey to all LAS users, through consistent policy statements, how information assets are to be safeguarded from unauthorised access, modification or deletion;
- Describe the required standards for the acceptable use of information systems and the requirements for accessing and disclosing information assets in accordance with regulations and applicable laws;

- Specify the minimum requirements that allow the LAS to avoid, detect, manage and recover from security incidents with the least disruption to the organisation;
- Ensure delivery partners, including offshore service providers, comply with LAS information security requirements and handle LAS data appropriately;
- Enable LAS to make the best use of its investment in ICT systems and enable the Trust to deliver a first rate service.

## 4 Responsibilities

### Trust Board

It is the role of the Trust Board to define the Trust's policy in respect of Information Security, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

### Senior Information Risk Owner (SIRO)

The SIRO is accountable to the Trust Board for Information Security and responsible for reporting Information Security risks to the Risk, Compliance and Assurance Group.

### Information Governance Group (IGG)

Chaired by the SIRO this Group will monitor the implementation of this policy.

### Caldicott Guardian

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

### 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.

### 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.

Line managers are responsible for notifying Human Resources when staff join, move or leave their teams and also for collecting any security badges, smart cards, laptops, mobile devices or any other equipment that were previously handed to their staff.

**All staff and third parties**

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

## 5 Policy Statement

### 5.1 Compliance

It is the policy of the LAS to ensure that:

a) Consistent security requirements are agreed and followed by all LAS functions and those organisations with which LAS shares information assets or allows access to its information systems;
b) Through a formal risk assessment and management programme there is an understood level of security for all valuable LAS assets such as IT systems, information assets, networks etc, thereby minimising the risks of compromising the confidentiality, integrity and availability of LAS information assets;
c) The confidentiality of information is maintained through a process of documented and managed access rights, i.e. protecting information from unauthorised disclosure and unauthorised access;
d) The integrity of information is preserved, i.e. by ensuring its accuracy and completeness through monitoring;
e) The availability of information, systems and services is maintained, i.e. by ensuring that information and LAS information systems are available to authorised users when required;
f) A combination of technical, procedural, personnel and physical security measures are used to protect end-user information (in particular personal information), LAS information assets and LAS information systems as required by the Data Protection Act (1998) and Human Rights Act (1998) from unauthorised access;
g) Measures are in place to protect LAS assets and LAS information systems from modification, damage or loss due to malicious software;
h) The Trust will ensure that business impact assessment, business continuity and disaster recovery plans are produced, maintained and tested for all mission critical information, applications, systems and networks;
i) Incident management procedures are established to ensure that:
    1 All security breaches or suspected breaches of information security are reported, recorded, investigated and resolved in a timely manner;
    2 All evidential data related to a security incident is collected, analysed, retained and presented in a manner consistent with the requirement to preserve evidential integrity, in order to support disciplinary and/or civil or criminal legal action that may occur as a result of the security incident. This requirement is in accordance with the requirement of the BIP 0008 British Standard.

j) Security education and awareness training is established, thereby ensuring that all LAS team members receive effective and regular training on the security policies and procedures adopted by LAS;
k) LAS communication facilities, including the use of Email, Internet, Intranet and radio, are used in efficient, effective, ethical and lawful manner (*see Appendix 1, Applicable Legislation*);
l) Personnel controls are applied to all LAS team members, temporary staff and contractors through recruitment checks;
m) Physical and environmental controls are enforced at all LAS locations where LAS information assets or LAS information has a presence, in order to prevent the unauthorised access, modification, loss or destruction of assets;
n) Any LAS information systems that handle Protectively Marked material are subject to regular risk assessment and where necessary, an accreditation process including security health checks to ensure the appropriateness of security measures;
o) Any LAS information assets that contain Protectively Marked material are protected in line with appropriate NHS or HMG policies, guidance, and procedures;
p) Mobile computing, communication and teleworking facilities are appropriately secured;
q) Contractual, regulatory and legislative requirements are met. A list of applicable legislation is attached as an Appendix 1 of this document;
r) Data retention procedures will be applied to ensure applicable systems are in compliance to statute and the Data Protection Act;
s) A continual process of improvement and compliance is applied to the management of information security within LAS (*see Appendix 2 for compliance statement for this document);*
t) When implementing security policy, the Trust will pay due regard to equality with the intent to eliminate discrimination, promote equal opportunities, promote good race relations and take account of disabled people's needs.
u) Changes to information systems, applications, or networks shall be reviewed and approved following Trust's Change Management and Third Party access policies and procedures.
v) Security will be incorporated into the specification of all new information systems or changes to existing systems.
w) All new information systems or enhancements should also provide user activity monitoring via appropriate audit trail mechanisms. Audit trail log files should be tamper-proof / of evidential integrity should they be required for submission in court and to stand up to non-repudiation. Manual records of user administration activity will be maintained for all current information systems that do not have electronic audit trail components. The Trust will ensure that all information systems are properly licensed and approved. Users can not install software on the Trust's property without permission
x) All internal or external confidential information transfers should be risk assessed. Only secure communication means should be

used to transfer confidential and personal information in compliance with the Trust's information governance/security policies and procedures and the Caldicott principles.

y) Removable, portable devices and media used to store, transfer or access confidential information must be encrypted.
z) Confidential or personal information (patient, staff or sensitive corporate data) must be disposed securely following Trust's secure disposal guidelines.

### 5.2 Security Monitoring

To ensure compliance with this policy statement and ensure the availability of critical services, LAS reserves the right to:

a) Monitor the use of LAS information systems and respond to concerns regarding alleged or actual violations of this policy, and, if necessary, take appropriate action;
b) Monitor and record access to LAS sites and premises using monitoring, access control and CCTV systems;
c) Monitor LAS communication systems and to enforce policies relating to the use of information and those communication systems;
d) Access an individual's information via electronic systems when that employee or user is not available.

## 6 Policy Exceptions

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

## 7 Further Information

Additional security policies contain details of how security must be applied to meet the requirements of this Policy. Additional security advice can be obtained from the IM&T Information Security Manager.

| IMPLEMENTATION PLAN | |
|---|---|
| **Intended Audience** | All staff and external |
| **Dissemination** | The Pulse and the LAS Website |
| **Communications** | Pulse feature |
| **Training** | No specific training, but an information security communication plan will be produced during 2012 |

**Monitoring:**

| Aspect to be monitored | Frequency of monitoring AND Tool used | Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported | Committee/ group responsible for monitoring outcomes/ recommendations | How learning will take place |
|---|---|---|---|---|
| Security breaches and serious incidents | An annual Information Governance Group meeting will be used to discuss compliance and appropriate actions for performance improvement e.g. change training content in light of experience. | Information Security Manager will monitor and report to IGG | Risk Compliance and Assurance Group will monitor outcomes and recommendations | Update training and awareness to reflect findings<br><br>Make policy changes to reflect new/ unforeseen circumstances |

**Appendix 1**

***Applicable Legislation***

It is LAS policy to fully comply with all applicable legislation and regulations, in particular, the following laws that are particularly applicable to information security.

- Official Secrets Act 1989
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- The Human Rights Act 1998
- The Equality Act 2010
- Privacy and Electronic Communications Regulations 2003 and 2004
- The Regulation of Investigatory Powers Act 2000
- The Interception of Communications Act 1985
- Electronic Communications Act 2000
- The Design Copyright and Patents Act 1988
- Police and Criminal Evidence Act 1984
- Crime and Disorder Act 1998
- Civil Contingencies Act 2004
- The Health and Safety at Work Act 1974
- The Lawful Business Practice Regulations 2000
- The Public Records Act 1958

**Appendix 2**

***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:

| | |
|---|---|
| Requirement 101 | There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda |
| Requirement 105 | There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans |
| Requirement 301 | A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed |
| Requirement 302 | There are documented information security incident / event reporting and management procedures that are accessible to all staff |
| Requirement 305 | Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems |
| Requirement 307 | An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy |
| Requirement 309 | Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place |
| Requirement 310 | Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error |
| Requirement 311 | Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code |
| Requirement 313 | Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely |
| Requirement 314 | Policy and procedures ensure that mobile computing and teleworking are secure |
| Requirement 323 | All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures |
| Requirement 603 | Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000 |