London Ambulance Service NHS Trust

Data Protection Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To provide a framework to manage Data Protection Act, 1998 requirements

.

Sponsor Department: Governance and Compliance

Author/Reviewer: Information Governance Manager. To be reviewed by May 2014.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
23/02/2011	2.3	Head RM	Further Revision
14/01/2011	2.2	Head RM	Revision
06/07/2010	2.1	Records Manager	Reformat
March 2007	2.0	Director IM&T	
March 2003	1.0	Director IM&T	

***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	27/05/11	3.0
	03/07	2.0
Chief Executive	03/03	1.0
Agreed by Trust Board (If appropriate):		

Published on:	**Date**	**By**	**Dept**
The Pulse			G&C
LAS Website			
Announced on:	**Date**	**By**	**Dept**
The RIB			G&C

EqIA completed on	**By**
21/03/11	C D-B; SM; BO
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
TP/048	LAS Information Security Policy	
TP/004	Complaints Procedure.	
TP/057	Waste Management Policy	
TP/022	Freedom of Information Policy	
TP/009	Policy for Access to Health Records, Disclosure of Patient Information, Protection and Use of Patient Information	
TP/017	LAS Procedure for Health Records	
TP/024	Managing Patient Confidentiality when Dealing with	

	the Media	
TP/029	Records Management & Information Lifecycle Policy	
	Information Commissioners Office guidance on Data Protection.- www.ic.gov.uk/guidance	
	Data Protection Act, 1998	
	Data Protection (Processing of Sensitive Personal Data) Order, 2000	
	Regulations of Investigatory Powers Act, 2000	
	Caldicott Review of Patient Identifiable information, 1997 / NHS Caldicott Manual, 2006	
	Computer Misuse Act, 1990	
	Access to Health Records Act, 1990	
	Directive on Privacy and Electronic Communications, 2002	
	The Privacy and Electronic Communications Regulations, 2003	
	Human Rights Act, 1998	

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 Data Protection Act 1998, (the Act), came into force on 1st March 2000 after receiving Royal Assent on 16th July 1998.

The Act repeals the Data Protection Act, 1984 and certain other legislation that gives rights of access to information held by organisations, including the Access to Personal Files Act, 1987.

The Act extends the rights given to individuals in previous legislation and requires data controllers (people or organisations that hold and process the details of living individuals) to comply with the Eight Principles (rules governing the use of personal data – see Appendix 1) and to bear in mind the rights and freedoms of those individuals when processing their details.

This document explains how the London Ambulance Service (LAS) will meet the legal requirements of the Act.

2. Scope

This policy covers all personal information that is stored in a relevant filing system.This policy is applicable to all staff, companies and other third parties holding, storing or using information for or on behalf of the LAS.

3. Objectives

1. To provide a framework to manage Data Protection Act, 1998 requirements.

2. To provide guidance to staff and third parties that explains the requirements of the Act and their responsibilities with regard to managing an individual's personal information.

4. Responsibilities

The **Chief Executive** has overall responsibility for ensuring that compliance with the Data Protection Act is managed responsibly within the Trust.

The **Director of Corporate Services** has strategic responsibility for Information Governance including compliance with the Data Protection Act throughout the Trust.

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

The **Assistant Director Corporate Services** has responsibility for the Governance and Compliance team which includes Information Governance.

The **Information Governance Manager** is responsible for the management of corporate processes concerning Data Protection including notification to the Information Commissioner.

The **Information Security Manager** is responsible for information security in the LAS and provides relevant support for data protection related issues.

The **Head of Patient Experiences** is responsible for the handling and processing of Subject Access Requests by the Patient Experiences Department made under the Data Protection Act.

The **Information Governance Group (IGG)** is chaired by the Director of IM&T who is the Senior Information Risk Owner (SIRO) and will monitor the implementation of this policy.

The **Senior Management Group** and **Heads of departments** are responsible for ensuring that the policy is implemented in their directorates and individual departments.

5. Enforcement

Any employee deliberately acting outside of their authority will be subject to LAS disciplinary procedures, up to and including dismissal where appropriate, and to possible legal action by the LAS. Any action to initiate legal proceedings shall be approved by any one of the Chief Executive, the Director (Human Resources) or the Director (Corporate Services).

6. Statement of Intent

The LAS intends to fulfil all its obligations under the Act. The LAS will ensure that the Information Commissioner is notified of all relevant processing and will conduct an annual review and update of the Notification Scheme to ensure that it remains up to date. It is the aim of the LAS that all appropriate staff are properly trained, fully informed of their obligations under the Act and are aware of their personal responsibilities.

The LAS will use the exemptions available to it to gather the necessary data to provide its patient care services to the public. It will share that information with other agencies, where it is legal to so do, if this enhances its ability to provide services that affect a person's health or where the LAS needs the support of another agency to ensure the best patient care for an individual. Any information sharing arrangements will be based upon formal protocols and will be in accordance with the Act's eight Data Protection principles (see Appendix 1). A pan-London information sharing protocol is under development.

The LAS will secure and maintain in accordance with the Act such data as is necessary to assist in the protection of the health and safety of its staff while continuing to comply with obligations to patients and others under the Act.

Individuals whose information is held and processed by the LAS can be assured that it will treat their personal data with all due care.

Where the LAS is not the data controller but rather the data processor it will abide by any written agreement between it and the data controller on data protection policy. This means where we process data collected by others. For example, Patient Transport Services (data processor) using information from a hospital trust (data controller).

This policy document applies only to information covered by the Act and will be updated as necessary according to the laws of the United Kingdom.

Separate codes of practice exist or are being developed within the LAS in respect of the following types of processing:-

- Personnel Data in Employer/Employee Relationships - including: access and disclosure of personal data, data matching, sensitive data, ethnic monitoring, and collection of personal data

- Security - including: CCTV, telephone, internet and e-mail usage, disposal of confidential waste, manual records and the security of buildings.

- TP/009 Policy for Access to Health Records - including patient access to their own records and the disclosure of Patient Information.

- TP/30 Records Management Retention and Disposal Policy and Procedure on the length of time records must be held.

7. Fair Obtaining/Processing

The LAS will, as far as is practicable, ensure that all individuals whose details it holds are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible and practicable, be informed of the likely recipients of the information – whether the recipients are internal or external to the LAS.

Processing within the LAS will be both fair and lawful and individuals will not be misled as to the uses to which the LAS will put the information given. If a person feels they have been deceived or misled as to the reason for which their information was collected, they should use the complaint process detailed at the end of this document.

Collection forms requiring personal information will contain a 'fair processing' statement giving details of who, why and for how long the information will be used. Where information is collected in person or by telephone, the employee asking for the details will tell the individual how those details will be used, who will use them and for how long the information will be kept. People are free to ask the person collecting the information why they want the details and what they will be used for. Please see the following example of a'fair obtaining' statement:

The information you have provided will only be held for the purposes of providing patient care, now or in the future, to you or to someone else on whose behalf you may be acting.

Where the LAS is using an exemption under the Act to obtain personal information that, in all of the circumstances, makes a fair obtaining statement impractical then no such statement will be made. Examples of this would be where:

- A 999 call taker needs to focus on collecting data that is time critical in order to protect the vital interests of an individual.

- A Paramedic/Technician is gleaning information from or about a patient and the care of that patient must take priority in the patient's own vital interests.

Any person identifiable information processed falls into one of two categories under the Act. These two types are personal data and sensitive personal data. Processing of these types of data require conformance with one set of conditions with regard to personal data and two sets of conditions when sensitive data is processed.

If a person's details are going to be used for automated processing (where a computer decides something based on a score or other information) the person will be entitled to be told about how the scoring system works and whether the decision can be challenged.

If a person's details are to be processed for a purpose that does not appear on the LAS's notification scheme (e.g. some new processing not previously notified) the individual will be given the information that would be necessary to make the processing fair and lawful. The LAS will undertake to make a formal notification to the Information Commissioner as soon as possible in these circumstances.

Any individual whose personal data (including photographs) are to be included on the LAS's web site will be asked to give their explicit consent. At the time of data collection, it will be made clear to individuals that details published on the LAS web site are viewable by anyone, anywhere in the world, who has access to the Internet.

8. Data Uses and Processes

The LAS will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of Data Protection law. Any new purposes introduced will, where appropriate, be notified to the individual and – if required by the law – their consent (see the Information Commissioner's guidance on 'consent') will be sought. A copy of the appropriate notification document is available from the LAS Information Governance Manager. The LAS Notification Scheme can also be viewed on the Information Commissioner's web page: www.dataprotection.gov.uk

All staff using personal data within the LAS will be told the limits of their authority to use and disclose such information through their managers, the induction process and training.

- All new purposes are documented and notified to the Information Commissioner.

9. Data Quality and Integrity

The LAS will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s). Details collected will be adequate for the purpose and no more. Information collected which becomes (over time or by virtue of changed purposes) irrelevant or excessive will be deleted. All of the LAS directorates/departments will manage data collection and updating of records such that accuracy, relevance, consistency with purpose and quality are assured.

Information will only be retained for as long as is necessary for the notified purposes(s) – after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will always be done within the requirements of the Act.. In some cases personal details will be removed from the record so that individuals cannot be identified.

The LAS will ensure, as far as is practicable, that the information held is accurate and up to date. It is the intention of the LAS to check wherever possible the details given. Information received from third parties (i.e. neither the individual concerned nor the LAS) will indicate the source, where practicable.

Where a person informs the LAS of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a comment will be placed on the disputed record indicating the nature of the problem. If the system does not allow the individual record to be marked in this way, departments will ensure that a manual record is made of the request and that it is processed within a reasonable time-scale.

Every effort will be made to reach an amicable agreement on any disputed data. Where this is not possible the LAS will implement its complaints procedure.

An internal investigation will be implemented if there is any alleged improper misuse of personal data by staff and appropriate action will be taken.

If a staff member suspects any weaknesses in the security of any information processing systems or suspects staff misuse with regard to data protection they should contact the Information Security Manager or Information Governance Manager as appropriate.

10. Technical and Organisational Security

The LAS has implemented appropriate security measures as required under the Act. These are set out in full in the LAS's Information Security Policy. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place and all LAS buildings have reception areas or controlled access.

Computer systems are installed with user-profile type password controls to ensure data is only accessed by authorised users, and where necessary, audit and access trails are monitored to establish that each user is fully authorised. In addition, all portable media is protected by encryption. Manual filing systems are held in secure locations and are accessed on a need-to-know basis only.

. The Information Governance Group regularly review Security arrangements and all reported breaches of security are investigated. Where necessary, further or alternative measures are introduced.

Where details need to be passed outside the LAS it will in general be done with the person's consent except where this is not possible or where it is required by law, i.e. the use of exemptions specified under the Act (such as crime prevention/detection, prevention of injuries etc.) or where it is in the person's vital interests. Any unauthorised disclosure will be dealt with under the LAS's disciplinary procedures.

Redundant personal data will be destroyed as confidential waste in line with TP/057 Waste Management Policy. In general, paper waste is shredded by outside certified contractors under local agreements and magnetic media (disks, tapes, etc.) are either electronically wiped or physically destroyed beyond recovery.

11. Subject Access/Subject Information Requests

The Act gives individuals the right to see information held about them and the same Act places a duty on the LAS to make that information available. Thus any person whose personal details are held/processed by the LAS has a right to receive a copy of his or her own information. There are a few exceptions to this rule (examples being data held for child protection, crime detection/prevention purposes or where the information is likely to cause serious harm to the physical and/or mental health of the patient or other individual) but most individuals will be able to have a copy of the data held about them.

Where any information relates to an identifiable third party, other than the data subject, consent must be gained from that third party, before any information relating to them can be released.

The LAS has the right to make a charge for such requests for computer based data and data held on paper or other media. An appropriate charge will be levied for this in line with the current LAS fees scheme.

Any codes used in the record will be fully explained; any inaccurate, out of date, irrelevant or excessive data will be dealt with under the procedures outlined in section 9 of this document, Data Quality and Integrity.

The LAS will reply to subject access requests as quickly as possible and in all cases within the 40 days allowed by the Act. Repeat requests will be fulfilled unless the period between is deemed unreasonable, such as a second request received so soon after the first that it would be unlikely for the details to have changed. The LAS will endeavour to fulfil all legitimate and reasonable requests. In some cases, especially with requests not submitted on the appropriate form, further information may be required from the requester which may delay the start of the 40 day maximum time limit.

12. Further Information, Enquiries and Complaints

The LAS Information Governance Manager is the first point of contact on any of the issues mentioned in this policy document. The Patient Experiences Department handles all internal and external enquiries. Where possible, requests for detailed information should be in writing.

Any complaints must be written, dated and must include details of the complainant as well as a detailed account of the nature of the problem. The LAS will attempt to complete internal investigations within twenty days and in every case the person will receive an acknowledgement as soon as possible after the complaint is received.

Complaints should be sent to the Patient Experiences Department who can be contacted by telephone on 020 3069 0240 or by writing to them at:

London Ambulance Service NHS Trust, St Andrews House, St Andrews Way, London E3 3PA.

IMPLEMENTATION PLAN	
Intended Audience	All LAS Staff
Dissemination	Available to all staff on the Pulse and to the public on the LAS website.
Communications	Revised Policy to be announced in the RIB and a link provided to the document.
Training	DP training is provided to new staff at Corporate Induction and to existing staff through a three year core training refresher course for support staff, online IG training and the IG section of a workbook for all operational staff. Staff who

	routinely handle DP SARS will receive more detailed training.
Monitoring	A quarterly and annual report will be completed by the Head of PED and IG Manager which describes activity, emerging themes and departmental performance. This will be made available to the Information Governance Group and Senior Managers Group to ensure corporate and departmental compliance with obligations. The annual report will also be made available to the Trust Board who will monitor outcomes/recommendations from the reports.

Appendix 1

The Data Protection Act, 1998: the eight principles

In order to process personal information in line with the Act, the following eight principles regarding privacy and disclosure must be satisfied.

First Principle

'Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- *at least one of the conditions in Schedule 2 is met; and*
- *in the case of **sensitive personal data**, at least one of the conditions in Schedule 3 is also met.'*

Second Principle

'*Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'*.

Third Principle

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'.

Fourth Principle

'*Personal data shall be accurate and, where necessary, kept up to date'*.

Fifth Principle

'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

Sixth Principle

'Personal data shall be processed in accordance with the rights of data subjects under this Act'.

Seventh Principle

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'.

Eighth Principle

'Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data'.

Appendix 2

Summary of Relevant Conditions for Processing Data

Schedule 2 Conditions

In all cases data controllers must satisfy at least one of the conditions in Schedule 2 of the Act. In the context of health sector data controllers, the most relevant Schedule 2 conditions are likely to be:

- Processing with the consent of the data subject;
- Processing necessary to protect the vital interests of the data subject;
- Processing which is necessary for the exercise of functions of a public nature exercised in the public interest by any person;
- Processing which is necessary for the purposes of the legitimate interests pursued by the data controller or those of a third party to whom the data are disclosed, except where the processing is prejudicial to the rights and freedoms or legitimate interests of the data subject.

When sensitive data is processed, at least one Schedule 3 processing conditions must be met. data. 'Sensitive data' is defined in the Act and includes data that relates to the physical or mental health of data subjects.

Schedule 3 Conditions

The most relevant Schedule 3 conditions are likely to be:

- Processing with the explicit consent of the data subject;
- Processing necessary to protect the vital interests of the data subject or another person, where it is not possible to get consent;
- Processing necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- The processing is necessary for medical purposes and is undertaken by a health professional or a person owing a duty of confidentiality equivalent to that owed by a health professional.

The Act provides that included within the term 'medical purposes' are preventative medicine, medical diagnosis, medical research, the provision of care and treatment, and the management of healthcare services. The

Commissioner considers that the term ‘vital interests’ refers to matters of life and death.

The Schedule 3 conditions have been supplemented by further conditions set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000.

The most likely conditions for health professionals would be:

- Processing of medical data or data relating to ethnic origin for monitoring purposes.

- Processing in the substantial public interest, necessary for the purpose of research whose object is not to support decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject and which is unlikely to cause substantial damage or substantial distress to the data subject or any other person.