London Ambulance Service NHS Trust

Data Protection Policy

Document Control

Document Reference	TP012
Version	v4.8
Approved by	Information Governance Group, Executive Committee
Lead Director/Manager	Chief Digital Officer
Author	Information Governance Manager
Distribution list	All Staff
Issue Date	1st April 2026
Review Date	1st April 2029

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To provide a framework to manage Data Protection legislation requirements

.

Sponsor Department: IM&T

Author/Reviewer: Information Governance Manager

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
March 2026	4.8	IG Manager	Minor Amends, Role Responsibilities, Data Use and Access Act 2025
October 2025	4.7	IG Manager	Minor Amendments
February 2025	4.6	IG Manager	Additional Legislation Added
February 2024	4.5	IG Manager	Review date amend.
February 2023	4.4	IS Manager	Minor Amendments
February 2022	4.3	IS Manager	Minor Amendments
19/07/22	4.2	IS Manager	Updated introduction scope, definitions, duties and responsibilities to incorporate IAO
14/07/22	4.2	IG Manager	Updated GDPR clauses reflective of latest legislation; now incorporates 'UK GDPR'

Contents

Introduction – Policy Objectives

Introduction

This policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards under the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) and Common Law Duty of Confidentiality.

The new DPA seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data. It supplements UK GDPR as well as extends data protection laws to areas which are not covered by UK GDPR. The DPA also ensures a single regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector. In order to comply with the DPA, information must be processed in accordance with the seven principles of the DPA. To comply with the General Data Protection Regulation (GDPR) EU 2016/679, information must be collected and used fairly, stored safely and not disclosed to any unauthorised person.

The DPA and UK GDPR legislates for the protection of personal information relating to living individuals. This applies to all information either manual or electronic that identifies a living individual (a natural person). The Access to Health Records Act 1990 will remain relevant for information relating to deceased persons.

Accountability is central to the DPA, Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

The Data Use and Access Act 2025 (DUAA) is a new Act of Parliament that updates some laws about digital information matters. It changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights.

Common law duty of confidentiality is not codified in an Act of Parliament but built up from case law through individual judgments. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.

The duty of confidentiality extends beyond death and is distinct from the obligations under the GDPR and DPA 2018.

The Trust also has a duty to comply with guidance issued by the Department of Health, NHS Digital, the NHS Executive, advisory groups to the NHS as well as guidance issued by professional bodies. These guidelines should not conflict with this policy or legislative requirements.

The Caldicott principles provide guidance on the use of and or transfer of personal information and the key recommendation out of the 16 in the Caldicott 2 report was that: “a senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information". The nominated individual is known as the Caldicott Guardian.

The National Data Guardian (NDG) standards set out 10 actions to be undertaken to assist in protecting information from loss, damage or inappropriate use.

The nature of the work undertaken by the Trust's employees, volunteers and contractors brings them into possession of a great deal of confidential and often highly sensitive information, both patient and staff related. Therefore, it is essential that the public at large have confidence that the organisation as a whole maintains confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose.

To provide a framework to manage Data Protection legislation requirements.

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

1. Scope and definitions

This policy covers all sites and systems operating and utilised by the LAS. It is applicable to all staff, volunteers, companies and other third parties holding, storing or using information for, or on behalf of, the LAS. It includes all data which is about a living individual and is held in any format including, but not exclusively, written and electronic.

This policy sets out how the Trust will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the DPA, UK GDPR, Data Use and Access Act 2025 and the Common law Duty of Confidentiality which are the key pieces of legislation covering security and confidentiality of personal information.

The Act applies to the processing of most forms of personal data including, but not exclusively, data held in the following which is not an exhaustive list:

- Databases
- Electronic filing systems (such as the H:\ and G:\ drives)
- Audit trails
- Emails and instant messaging
- Spreadsheets
- Word processing documents
- Paper Files / filing systems
- CCTV
- Audio and Video recordings
- Photographs and scans
- X-ray, CT, MRI
- Portable Media, memory sticks, disks, phones, cameras
- Payment system
- SharePoint

This policy also applies to non-patient personal data such as that of Staff and volunteers, charity workers, staff holding a letter of access. This is not an exhaustive list. Such personal data may include for example personnel records and occupational health records, contact details for newsletters or charitable activities.

The Trust as a "Data Controller" is responsible for all records detailed above.

The Policy applies to:

- All information used by the Trust;
- All information systems managed by or for the Trust;
- Any individual using information 'owned' by the Trust;
- Any individual requiring access to information 'owned' by the Trust
- Any individual working on behalf of the Trust, or anyone who accesses Trust premises and information which is owned or managed by the Trust.

Definitions:

Word / Term	**Definition**
Data Controller	The legal person, or organisation, which determines the purpose and means of the processing of personal data. The Trust is a data controller.
Data Processor	The legal person, or organisation, which processes personal data on behalf of the controller.
Data Subject	The identified or identifiable living individual to whom personal data relates. A data subject can be a patient but also a member of staff who's personal information is held by the Trust.
Identifiable living individual	Living individual who can be identified, directly or indirectly, in particular by reference to: • an identifier such as a name, an identification number, location data or an online identifier; or • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Information Commissioner	Independent regulator set up to uphold information rights.
Personal data	Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (see section 8 for special category data).
Processing	In relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

	• collection, recording, organisation, structuring or storage; • adaptation or alteration; • retrieval, consultation or use; • disclosure by transmission, dissemination or otherwise making available; • alignment or combination; or • restriction, erasure or destruction.
Accessible Public Record	Records kept by a public body such as the Trust and covered by the Public Records Act 1958 and 1967.
Anonymised Data	Data from which the identity of an individual cannot be determined. Anonymisation requires the removal of name, address, full post code and or image, or some other unique personal characteristic.
Biometric	Biometrics are body measurements and calculations related to human characteristics. Biometric authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or finger prints.
Caldicott Principles	The eightCaldicott Principles relating to the use of patient identifiable information are: • Justify the purpose(s) of using confidential information • Only use it when absolutely necessary • Use the minimum that is required • Access should be on a strict need-to-know basis • Everyone must understand his or her responsibilities • Understand and comply with the law • The duty to share information can be as important as the duty to protect patient confidentiality. • **Inform patients and service users about how their confidential information is used**

CCTV	Closed Circuit Television
Code of Practice	A set of documented procedures used by public bodies to ensure they comply with legislation. For example, the NHS code of confidentiality.
Common Law Duty of Confidentiality	A law which is determined by decisions made by the courts and can therefore change over time. A law set by precedents.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Confidential Information	Confidential information could include, without limitation details of: Business Contacts, associates, list of suppliers and details of contract with them. Identities of patients, expenditure levels and Trust specific pricing policies. Proposal plans or specification for the development of existing services and of new services. Details of employees and officers of the Trust and of the remuneration and other benefits paid to them. Presentations, tenders, projects, joint ventures, mergers and developments contemplates, offered or undertaken by the Trust.
Consent	Consent is the fact that permission has been given. A person who consents to something is, in effect, giving permission for that thing to happen.
Explicit or Express Consent	This means the individual has given a clear, unambiguous agreement for their data to be used in a specific way, either orally or in writing. Both terms are used to describe circumstances where a clear and voluntary preference or choice, is given. It must be given freely in circumstances where the available options and the consequences have been made clear.
Data	A collection of facts from which conclusions may be drawn; "statistical data".
Data Protection Act 2018 (DPA)	UK wide legislation that governs the use of personal information. Its purpose is to protect the right of the individual. The Act laid down seven data protection principles.
Destruction	Process of eliminating or deleting records, beyond any possible reconstruction.
Disclosure	The release of personally identifiable data to a third party.

Fair Processing	Fairness means handling personal data in a way individuals expect and not using it in ways that lead to unjustified adverse effects. You must consider the fairness of your processing, including the ways in which information about them may be collected and used.
Filing System	Means any structured set of personal data which are accessible accordingly to specific criteria, whether centralised, decentralised on functional or geographical basis.
Genetic Data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
Health Record	"health record" means a record which— (a) consists of data concerning health, and (b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates; This includes mental or physical health. The definition also applies to Occupational Health Records. Thus, with the exception of anonymised information, most if not all NHS information concerning patients, whether held electronically or on paper, will fall within the scope of the Act.
Information Sharing Protocol	(ISP) Data Sharing Agreement (DSA)- Documented rules and procedures for the disclosure and use of patient or other individual's personal information between two or more organisations or agencies. Sharing agreements must be in place before the sharing takes place.
Security Logs	Security logs are information regarding the security related events that happen on a system and may consist of records (text files) that are created automatically during system operation and contain entries about the events that happened in a system.
Manual Data / Records	Information that is not processed by means of equipment.
Medical Purposes	As defined in the Data Protection Act 2018, means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

NHS Code of Confidentiality	A guide to required practice for those who work within or under contract to NHS organisation concerning confidentiality and patients' consent to the use of their health records.
Personal Data	"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Profiling	Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymised Information	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. The additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person, whilst still being categorised as identifiable data.
Public Interest	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.
Research	Research – the attempt to derive generalisable new knowledge including studies which aim to generate hypotheses as well as studies that aim to test them https://www.hra.nhs.uk/planning-and-improving-research/research-planning/access-study-support-advice-services/
Restriction of Processing	The marking of stored personal data with the aim of limiting their processing in the future.
Special Category Data	• personal data revealing **racial or ethnic origin**; • personal data revealing **political opinions**;

	• personal data revealing **religious or philosophical beliefs**; • personal data revealing **trade union membership**; • **genetic data**; • **biometric data** (where used for identification purposes); • data concerning **health**; • data concerning a person's **sex life**; and • data concerning a person's **sexual orientation**.
Data relating to criminal offences and convictions	Are addressed separately under the Law Enforcement Directive of the Data Protection Act 2018. Any information that is being processed for law enforcement purposes must adhere to the governance requirements of Part 3 of the DPA 2018. These include logging requirements, categorisation and obligations about the principles and rights of individuals.
Special Purposes	A term used in the Data Protection Act 2018. It refers to data used for the purposes of: (a) the purposes of journalism; (b) academic purposes; (c) artistic purposes; (d) literary purposes.

2. Accountabilities and Responsibilities

a. The **Trust Board** is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives. The Trust as a body corporate is a data controller.

b. The **Chief Executive** has overall accountability and responsibility for Information Governance and is required to provide assurance that all data protection risks are effectively managed and mitigated, for ensuring that compliance with Data Protection legislation is managed responsibly within the Trust.

c. The **Caldicott Guardian** is responsible for protecting the confidentiality of patient and service-user information and this policy supports the Caldicott function. They are responsible for promoting and ensuring that the Caldicott principles are followed and that sharing of patient information is facilitated as appropriate. The Caldicott Guardian must maintain a strong knowledge of confidentiality and data protection law and oversee arrangements where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.

Caldicott Guardians must be registered with the UK Caldicott Guardian

Council. The register is maintained by NHS Digital.

d. The **Chief Digital Officer** is also the Senior Information Risk Owner (SIRO) and has strategic responsibility for Information Governance including compliance with the Data Protection Act throughout the Trust.

The SIRO has ultimate responsibility for the management and mitigation of risks associated with the Trust's information management processes and chairs the Information Governance Group. The Senior Information Risk Owner (SIRO) should be an Executive Director or other senior member of the board.

The key responsibilities of the SIRO are to:

- Take ownership of the risk assessment process for information and cyber security risks.
- Review and agree action in respect of identified information risks.
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues.

The SIRO ensures that identified information security incidents/risks are followed up and incidents managed. They ensure that the Board is briefed on all GDPR issues. The role is supported by the Trust's Data Protection Officer and Deputy SIRO.

e. The **Data Protection Officer** is responsible for providing specialist data protection advice and for developing specific guidance notes on data protection issues, and has responsibility for confidentiality and security issues for all patients and staff. The DPO is responsible for ensuring payment of administrative fees in respect of the legislation to the Information Commissioners Office (ICO). The DPO also has the responsibilities laid out in Article 39 of the UK GDPR – see Appendix 1.

The DPO must be independent and cannot be instructed as to the content of the advice given. They have oversight of investigations and reports to the ICO all breaches within 72 hours. They should provide advice on the completion of data privacy impact assessments (DPIA's) and whether a DPIA is required for the given processing. The data controller and the processor must involve the DPO fully and at the earliest point in all issues which relate to the processing of personal data.

f. The **Information Governance Manager** provides specialist knowledge in management leadership for information governance and has responsibility for

leading the strategic development of policies, procedures and standards relating to information governance. It is their responsibility to raise awareness and acceptance of information governance standards, with the aim of enabling information into the organisation. While working closely with the SIRO and Caldicott Guardian, they must investigate and advise on Information Governance security issues including breaches and other information governance incident reports. Ensuring that that the Trust's activities consistently support accountability, openness, fairness and transparency of process.

They are the first point of contact for the ICO in relation to data processing. They must ensure that the Trust's business activities are conducted in a manner consistent with the data protection act 2018, the UK General Data Protection Regulation (UKGDPR) and Freedom of Information Act 2000. They are also responsible for the management and yearly submission of the DSPT assurance assessments. This includes monitoring compliance levels and monitoring the development of legislation and guidance as it affects the use of information within the Trust.

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

The Information Security Manager must:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Be accountable to the SIRO and other bodies for Information Security across the Trust.
- Work with the Trust IG Manager to monitor potential and actual security breaches with appropriate expert security resource.
- If a security incident or risk occurs or is found, the Information Security Manager is to follow the correct escalation process as outlined in the Trust Data Protection Policy.
- Where this post is not resourced or established a third party or serviceprovider may fulfil these duties.

h. The **Head of Patient Experience** is responsible for the handling and processing of Subject Access Requests by the Patient Experiences Department made under the legislation.

i. The **Head of Workforce Analytics** is responsible for coordinating the handling

of Subject Access Requests received from staff and ex-staff.

j. The **Information Governance Group (IGG)**, chaired by the Senior Information Risk Owner (SIRO), and Deputy Chair is the Caldicott Guardian, will monitor the implementation of this policy.

This Group's mandate covers all elements of Information Governance and consequently deals with all issues of compliance and acts as a point of reference for queries and problems raised by staff, patients and others. This group will also be responsible for completion of the annual assessment against the DSPT, developing annual improvement plans, monitoring progress on implementing those plans and reporting to the Trust Board. The activity of the IGG will be reported regularly to the Risk, Compliance and Assurance Group (RCAG).

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

l. **Information Asset Owners** (IAO) will ensure that:

- All information assets are documented and kept appropriately secure, in line with the Data Protection Act Principles and are not kept for longer than necessary.
- Information Asset Owners will be supported by Information Asset Administrators, but the overall responsibility for the management of the Trust information assets sit with the Information Asset Owners.
- Information Asset Owners (IAO's)/Information Asset Administrators (IAA's)/are appointed for all departmental databases/information systems and their details notified in writing to the Information Governance Manager | DPO via the Information Security Officer
- Appropriate local systems are in place regarding manual files held in the department that contain personal details (typically patient or staff records)
- Information is used for the purposes declared and that it is maintained and disposed of in accordance with Trust policies.
- Systems are in place to check the accuracy of personal data held in their departments about staff or patients
- The responsibility for the legal basis for processing personal information is with the IAO which they must ensure is kept up to date.
- Ensure annual flow mapping is completed ensuring each instance of processing is identified and documented (including as appropriate, Sharing agreement, processing agreement, Contract and DPIA.)

m. **All employees Including voluntary workers)** of the Trust, which includes staff working as contractors, temporary staff and students, who record/process personal data must ensure that they comply with the requirements of the GDPR. Any personal data should be kept securely. Personal data must not be disclosed verbally or in writing or otherwise to any unauthorised third party. A breach of the GDPR or the Trust's Data Protection Policy may result in disciplinary proceedings. Contact the Head of Information Governance for data protection advice when unsure.

3. Policy Content Data Protection Legislation

Common Law of Confidentiality

The Common Law of Confidentiality is created by judicial precedent rather than Act of Parliament, that 'information confided should not be used or disclosed further, except as originally understood by the confider or with their subsequent permission'.

Generally, if a data subject's information is disclosed in circumstances where it is expected that a duty of confidence applies, it should not normally be disclosed further without that data subject's consent.

There should be no use or disclosure of any confidential patient information for any purpose other than the direct clinical care of the patient to whom it relates, in which case implied consent is used, however there are some exceptions.

- The patient explicitly consents to the use or disclosure.
- The disclosure is required by law, or the disclosure is permitted under a statutory process that sets aside the duty of confidentiality.
- The disclosure can be justified in the public interest.

Data Protection Act 2018

a. The 2018 Data Protection Act (DPA) assists with and supplements the adoption of the UK GDPR into UK law. It strengthens or provides exceptions from some of the requirements of the UK GDPR and also extends data protection law into types of processing that are not covered by the UK GDPR.

b. The DPA provides the Information Commissioner with additional functions and introduces new powers and offences in relation to data protection. The DPA applies to staff as well as patient records and covers both paper and electronic records.

c. Any individual has the right to see what information is held about them and may challenge this information if they feel it is inaccurate or has caused damage to them. The DPA places obligations on those who record and use information about individuals. They must register the use of that information and they must ensure that they follow sound practices in recording and using the information.

Data Protection Principles (UKGDPR)

Article 5 of the UK GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Use and Access Act 2025

The DUAA is a new Act of Parliament that updates some laws about digital information matters. It changes data protection laws in order to promote innovation and economic growth and make things easier for organisations, whilst it still protects people and their rights.

The Act does not replace the UK GDPR, Data Protection Act 2018 or the Privacy and Electronic Communications Regulations 2003. Instead, it makes some changes to them to:

- make the rules simpler for organisations
- encourage innovation
- help law enforcement agencies to tackle crime, and
- allow responsible data-sharing while maintaining high data protection standards.

Lawful basis for processing

There must be a valid lawful basis in order to process personal data. With the introduction of the DUAA, there will now be seven available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

The lawful basis must be determined and documented before processing. The LAS privacy notice will include the lawful basis for processing as well as the purposes of the processing. Processing of special category data requires both a lawful basis for general processing and an additional condition for processing.

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever personal data is processed:

- Consent: the individual has given clear consent to process their personal data for a specific purpose.

- Contract: the processing is necessary for a contract with the individual, or because the individual has asked the LAS to take specific steps before entering into a contract.

- Legal obligation: the processing is necessary for the LAS to comply with the law (not including contractual obligations).

- Vital interests: the processing is necessary to protect someone's life.

- Public task: the processing is necessary for the LAS to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

- Processing is necessary for the purposes of a recognised legitimate interest (Additional lawful basis under DUAA)

- Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply to public authorities processing data to perform official tasks.)

Special category data

d. When processing special category data it is necessary for the LAS to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. We will document both our lawful basis for processing and our special category condition so that we can demonstrate compliance and accountability.

e. Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

f. This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. The choice of lawful basis under Article 6 does not dictate which special category condition must be applied, and vice versa. For example, if consent is used as the lawful basis, there is no restriction to using explicit consent for special category processing under Article 9. The most appropriate special category condition in the circumstances should be chosen – although in many cases there may well be an obvious link between the two. For example, if the lawful basis used is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

g. The conditions are listed in Article 9(2) of the UK GDPR:

(a) the data subject has given explicit consent to the processing of their personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not- for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

processing is necessary for the establishment, exercise or defence of legal claims

or whenever courts are acting in their judicial capacity;

processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health
care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Individual Rights

h. The UK GDPR provides the following rights for individuals:
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

i. The lawful basis for processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	×
Contract	✓	✓	×
Legal obligation	×	×	×
Vital interests	✓	×	×
Public task	×	×	✓
Legitimate interests	✓	×	✓

j. However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies. The remaining

rights are not always absolute, and there are other rights which may be affected in other ways.

Personal Data Breaches

k. The LAS is required to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individual must also be informed without undue delay. The LAS will maintain records of any personal data breaches in the RADAR system regardless of whether we are required to notify.

   A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

   Personal data breaches can include:

   - access by an unauthorised third party;
   - deliberate or accidental action (or inaction) by a controller or processor;
   - sending personal data to an incorrect recipient;
   - computing devices containing personal data being lost or stolen;
   - alteration of personal data without permission; and
   - loss of availability of personal data.

All staff are responsible for recording all actual and near miss incidents involving any aspect of Information Governance within 24 hours. They will report Information incidents on RADAR, alerting the Information Governance Manager. Incidents will be categorised by type and local management teams will follow these up as appropriate. The Information Governance Manager will then assess the incident and determine whether or not the incident needs to be notified to the ICO (within 72 hours).

Third party contractors, partners or provider organisations are required to notify LAS immediately if a breach, or suspected breach, occurs that may involve LAS information. The Information Governance Manager will again assess the incident and determine whether or not the incident needs to be notified to the ICO (within 72 hours).

Accountability and Governance

l. Under the legislation the LAS is responsible for complying with the UK GDPR and must be able to demonstrate compliance. We will:

   - Put in place appropriate technical and organisational measures to meet the requirements of accountability.
   - Adopt and implement data protection policy and procedural documents.

- Take a ‘data protection by design and default’ approach.
- Put written contracts in place with organisations that process personal data on our behalf.
- Maintain documentation of processing activities.
- Record and, where necessary, report personal data breaches.
- Carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests.
- Appoint a data protection officer.

m. The obligations that accountability places on the LAS are ongoing. It is not simply signing off a particular processing operation as ‘accountable’ and moving on. Measures implemented must be reviewed at appropriate intervals to ensure that they remain effective and updated when required.

n. The LAS must be able to show that it has considered the risks to personal data and put in place measures and safeguards to provide mitigation against any potential data breaches.

Statement of Intent

o. The LAS intends to fulfil all its obligations under existing legislation including ensuring that its registration details with the ICO are accurate and up to date. The LAS will secure and maintain in accordance with the legislation 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 legislation.

p. 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.

Privacy by Design

q. As required by the legislation all new projects and initiatives will be checked to ensure that wherever personal data is involved a Data Privacy Impact Assessment is carried out to document the measure put in place to protect personal data. This is documented in TP059 Data Privacy Impact Assessment Policy and Procedure.

Privacy Notices

r. 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 whose information is held and processed by the LAS can be assured that it will treat their personal data with all due care and Privacy Notices will be provided to show the LAS use of personal data and the legal basis for processing.

s. 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. There is a Privacy Notice on the LAS website which states ‘How we use your personal information’.

Information Sharing

t. The LAS will share personal 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. Where required information sharing arrangements concerning Patient Confidential Data (PCD) will be based upon formal protocols and information sharing agreements which will document the legal basis for sharing.

Data Quality and Integrity

u. The LAS will not collect data from individuals where that information is excessive or irrelevant in relation to the 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.

v. Information will only be retained for as long as is necessary 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 legislation. In some case's personal details will be removed from the record or pseudonymisation will be used so that individuals cannot be identified.

w. 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.

x. 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.

y. 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.

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

aa. 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 Data Protection Officer.

Technical and Organisational Security

bb. The LAS has implemented appropriate security measures as required under the legislation. 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.

cc. 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.

dd. The Information Governance Group will review security arrangements and reported breaches of security. Where necessary, further or alternative measures will be introduced.

ee. Where details need to be passed outside the LAS it will be done a required by the legislation. Any unauthorised disclosure will be dealt with under the LAS's disciplinary procedures.

ff. Redundant personal data will be destroyed as confidential waste in line with TP057 Waste Management Policy. In general, paper waste is shredded internally by cross-cut shredders or by outside certified contractors under local agreements and magnetic media (disks, tapes, etc.) are either electronically wiped or physically destroyed beyond recovery.

Subject Access/Subject Information Requests

gg. The legislation gives individuals the right to see information held about them and it 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 without payment of a fee. 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.

hh. 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.

ii. 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 0 of this document, Data Quality and Integrity.

jj. Subject access requests from the public or solicitors acting on behalf of the public will be handled by Patient Experiences Department; those from the police will be handled by Operational Information and Archives; those from staff and ex-staff will be handled by the Workforce Team.

kk. The LAS will reply to subject access requests as quickly as possible and within the 30 days (one month) allowed by the legislation unless the request is of a complex nature. Repeat requests will be fulfilled unless the period between is deemed unreasonable, that is less than six months, 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 case's further information may be required from the requester which may delay the start of the 30 day maximum time limit.

Further Information, Enquiries and Complaints

ll. The LAS Data Protection Officer is the first point of contact on any of the issues mentioned in this policy document. The Patient Experiences Department handles all external complaints. Where possible, requests for detailed information should be in writing.

mm. Any complaints must be managed in accordance with the Trust's complaint procedure: written, dated, and include details of the complainant as well as a detailed account of the nature of the problem. The LAS will aim to provide a substantive response within twenty-five working days and in every case the person will receive an acknowledgement within three working days of the complaint being received.

nn. Complaints should be sent to the Patient Experiences Department who can be contacted by telephone on 020 3069 0240 or by email: Londamb.patient.experiences@nhs.net

Enforcement

oo. 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 either the Chief Executive, or the Director of Corporate Governance.

4. Implementation Plan

IMPLEMENTATION PLAN				
Intended Audience	All LAS Staff			
Dissemination	LAS Connect			
Communications	Internal Communications			
Training	DP training is provided to new staff at Corporate Induction and to existing staff by annual online IG training. See also S.5 of this policy.			
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**
Compliance with the Act through review of incidents	Quarterly through reports such as briefing papers	DP Officer, Information Governance Group	RCAG	Revision of policy and training.

5. Competence (Education and Training

It is a requirement that all staff complete their annual mandatory Information Governance training in accordance with the Data Security and Protection Toolkit. It is important for all staff to be properly trained, fully informed of their Data Protection obligations and are aware of their personal responsibilities.

The LAS Confidentiality Code of Conduct outlines the obligations of all staff to ensure that access to personal data is appropriate, kept secure and not disclosed to unauthorised persons

6. Monitoring Compliance

The Information Governance Group will be responsible for leading on the

implementation of this policy and other Information Governance related policies and procedures. It will ensure that clear formal guidelines have been provided to staff on all aspects of Information Governance.

The review or creation of other Information Governance related policies and procedures will include mechanisms for monitoring compliance with this policy or other procedure standards.

This policy will be continually monitored and will be subject to regular review, an early review may be warranted if one or more of the following occurs:

- As a result of regulatory / statutory changes or developments
- As a result of NHS policy changes or developments
- For any other relevant or compelling reason

7. Policy Review

This policy will be reviewed every three years or earlier if there are changes to National Guidance or significant changes to the management of risk across the organisation.

8. Equality Impact Assessment Statement

The Data Protection Policy Framework and associated guidance and checklists provide an accessible process and level of support to enable everyone to constructively resolve any issues that they have.

9. References

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	
TP080	Social Media Policy	
	Information Commissioners Office guidance on Data Protection.- www.ic.gov.uk/guidance	
	Data Protection Act 2018	
	Regulations of Investigatory Powers Act, 2000	
	The Information Governance Review (Caldicott 2) 2013 and Caldicott 3)	
	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	

Appendix 1 Article 39 – Tasks of the DPO

The data protection officer shall have at least the following tasks: a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(a) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(b) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(c) to cooperate with the supervisory authority;

(d) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.