The London Ambulance Service NHS Trust Privacy Notice for the purposes of employment and staffing.

This privacy notice tells you what to expect us to do with your personal information when you contact us or use our services as an employee, volunteer, ex-employee, agency staff, contractor, seconded staff or non-executive director.

You can find more detailed information about how we your information for the following specific purposes here:

- Main privacy notice – Privacy Notice - London Ambulance Service NHS Trust
- Research within the LAS – **https://www.londonambulance.nhs.uk/about-us/research/#**
- Cookies – https://www.londonambulance.nhs.uk/privacy-policy/

Our contact details

Name: London Ambulance Service NHS Trust

Address: Headquarters: Waterloo

220 Waterloo Road
London
SE1 8SD

Our telephone number is 020 7783 2000.

- General Information Governance/Data Protection inquiries email address: londamb.ig@nhs.net

- Website: https://www.londonambulance.nhs.uk/

- We are the controller for your information. A controller decides on why and how information is used and shared

Data Protection Officer contact details

- Our Data Protection Officer is Philip John, who is also our Information Governance Manager, and is responsible for monitoring our compliance with data protection requirements. You can contact him with queries or concerns relating to the use of your personal data at philip.john1@nhs.net

As an employer, the London Ambulance Service (LAS) must meet its contractual, statutory and administrative obligations. We are committed to ensuring that the personal data of our employees is handled in accordance with the principles set out in the Data Protection Act (DPA) (2018) and UK General Data Protection Regulations (UK GDPR).

This privacy notice tells you what to expect when the LAS collects personal information about you. It applies to all employees, volunteers, ex-employees, agency staff, contractors, seconded staff and non-executive directors. However the

information we will process about you will vary depending on your specific role and personal circumstances.

How do we get information and why do we have it?

The personal information we collect is provided directly from you for one of the following reasons:

- Directly from you.
- From an employment agency.
- From your employer if you are seconded.
- From referees, either external or internal.
- From security clearance providers.
- From Occupational Health and other health providers.
- From Pension administrators and other government departments, for example tax details from HMRC.
- From your Trade Union.
- From the Car Parking Scheme.
- From providers of staff benefits.
- CCTV images from our landlords or taken using our own CCTV systems.

What information do we collect?

Personal information

We currently collect and process the following personal information:

Names; dates of birth; NHS numbers; National Insurance numbers: addresses, email addresses, telephone numbers and IP addresses if you contact us over the website.

More sensitive information

We currently collect and process the following more sensitive data (including special category data):

- Data concerning physical or mental health data.
- Data revealing racial or ethnic origin.
- Data concerning a person's sexual orientation.
- Biometric data (where used for identification purposes).
- Data revealing religious or philosophical beliefs.
- Data revealing political opinions.
- Data revealing trade union membership.
- Data relating to criminal or suspected criminal offences.
- Data concerning marital status and next of kin details.

Who do we share this information with?

Information related to your employment

We use the information to carry out the contract we have with you, provide you access to business services required for your role and manage our human resources processes. We will also use it for our regulatory purposes in our role as a supervisory authority.

- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses.
- Your date of birth, gender and National Insurance number.
- A copy of your passport or similar photographic identification and / or proof of address documents.
- Marital status.
- Next of kin, emergency contacts and their contract information.
- Employment and education history including your qualifications, job application, employment references, right to work information and details of any criminal convictions that you declare to us.
- Location of employment (e.g. Waterloo, London and / or other regional offices).
- Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations.
- Security clearance details including basis checks and higher security clearance details according to your job.
- Your responses to staff surveys if this data is not anonymised.
- Your political declaration form in line with our policy and procedure regarding party political activities.

Information related to your salary, pension and loans

We process this information for the payment of your salary, pension and other employments related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave.

- Information about your job role and your employment contract including; your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working).
- Details of your time spent working and any overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets.
- Details of any leave including sick leave, holidays, special leave
- Pension details including membership of both state and occupational pension schemes (current and previous).
- Your bank account details, payroll records and tax status
- Trade Union membership for the purpose of the deduction of subscriptions directly from
- Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1

forms/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking.

Information relating to your performance and training

We use this information to assess your performance, to conduct pay and grading reviews and to deal with any employer / employee related disputes. We also use it to meet the training and development needs required for your role.

- Information relating to your performance at work e.g. probation reviews, PDRs.
- Grievance and dignity at work matters and investigations to which you may be a party.
- Disciplinary records and documentation related to any investigations, hearings and warnings/penalties.
- Whistleblowing concerns raised by anyone who works (or has worked) in the NHS, or for an independent organisation that provides NHS services can raise concerns. This includes agency workers, temporary workers, students, volunteers and Board.

Information relating to monitoring.

We use this information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees.

- Information about your access to data held by us for the purposes of criminal enforcement if you are involved with this work.
- Information derived from monitoring IT Acceptable Use Standards.
- Photos, body worn camera videos and CCTV images.

Information relating to your health and wellbeing and other special category data

We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees.

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e. Statement of Fitness for Work from your GP or hospital.
- Accident records if you have an accident at work.
- Details of any desk audits, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, gender identification and may be extended to include other protected characteristics.

Information relating to surveillance cameras, CCTV, (Crew Safety System inclusive of CCTV & Body Worn Cameras)

The London Ambulance Service utilises surveillance cameras (Static/Vehicle based CCTV and Body Worn Cameras) in and around the Trust's sites, on our emergency vehicles, as well as body worn cameras used by operational crews which has been rolled out nationally following a successful local pilot.

Please note: Our surveillance cameras inside our vehicles and our body worn cameras are only activated by the crew when they feel there may be a risk to safety. Should these systems be activated, the crew will advise you and/or an audio message will be played inside the vehicle with a recording flashing light on the body worn cameras.

Using call recordings for safety campaigns

To help protect our colleagues and the public, London Ambulance Service may occasionally use short extracts from calls in safety and awareness campaigns. These campaigns aim to explain the impact of abusive or inappropriate behaviour and encourage people to treat our colleagues with respect.

Any extract used publicly will be anonymised. We will remove names, contact details, locations, clinical information and other details that could identify the caller, patient or anyone else involved. Voices will also be altered where necessary and only the minimum amount of audio needed will be used. Identifiable recordings will not be published.

Automation, Ambient Voice Technology and Artificial Intelligence

The London Ambulance Service is committed to providing high-quality care while ensuring the privacy and confidentiality of your personal information. As part of our ongoing efforts to enhance patient care, we are assessing and adopting a number of advanced technology solutions, including Automation Technology, Ambient Voice Technology and Artificial Intelligence tools to support the service we provide.

These Tools include, but are not limited to:

- **TORTUS** - A medical AI ambient voice application designed to streamline clinical documentation by both transcribing patient conversations in real-time and allowing clinician dictation, to support drafting of medical notes, letters, and coding suggestions. As with any digital products involving patient information, this product is subject to strict governance arrangements including MHRA regulation. Clinicians always check and validate records created with the support of AI.

- **Copilot** – Microsoft's Enterprise 365 Copilot is a generative AI product. It automatically inherits the existing security, compliance, and privacy policies for Microsoft 365. Microsoft 365 Copilot processes data without storing it. User data is not used to 'retrain' the Copilot large language model. Results are returned from Copilot to the user, and are provided for the user to choose to use or disregard. Copilot only processes patient data to conduct thematic reviews of trends via patient surveys and is outputted in aggregated, non-identifiable outputs only. It may only be used to process staff data in approved situations. In all use cases LAS will ensure correct governance is in place.

- **Blue Prism** – Automated task processing application that is currently deployed to support staff in accessing organisational and policy information within the organisation.

How we use or plan to use Automation, Ambient Voice Technology and Artificial Intelligence tools:

- Enhanced Care: Automation, Ambient Voice Technology and Artificial Intelligence technology to assist our healthcare professionals in delivering efficient and effective care. This includes supporting clinical decision-making and improving the efficiency and content of medical records.
- Data Processing: The Automation, Ambient Voice Technology and Artificial Intelligence tools may process personal, special category, and confidential data. This processing is conducted in line with the reasonable expectations of our patients and complies with data protection laws.
- Privacy and Security: We ensure that all data processed by Automation, Ambient Voice Technology and Artificial Intelligence tools are handled securely and confidentially. Our systems are designed to protect your information and uphold your rights under the UK Data Protection Act 2018 and GDPR. In cases where an Automation, Ambient Voice Technology and Artificial Intelligence tools are implemented within the Trust they will only be approved following the completion of a Data Protection Impact Assessment.
- Transparency: We are committed to transparency about how your data is used. If you have any questions or concerns about the use of AI technology in your care, please do not hesitate to contact us.

Automated Decision-Making

We may use your information to support automated decision-making alongside human involvement. These automated systems may have a significant potential impact. Examples include systems to communicate concerns around safeguarding and those involved in ensuring the earliest possible dispatch of ambulances for the highest priority emergencies. In cases where automated decision-making is implemented within the Trust, it will only be approved following the completion of a Data Protection Impact Assessment, and will also be subject to UK GDPR regulations regarding the rights of individuals relating to automated decision-making.

Lawful Basis for how we use Automation, Ambient Voice Technology and Artificial Intelligence tools

The lawful basis to process your personal data does not change because we use Automation, Ambient Voice Technology and Artificial Intelligence tools and can be viewed under the 'What is our Lawful Basis for using information' section of this Privacy Notice.

Ambulance Data Set

We routinely collect information from the initial contact when we receive a call in the 999 Emergency Operations Centre (EOC) through to completing an electronic patient record (EPR) with information about the patient and care we provide, when we attend an incident. Some of this information goes on to form part of the Ambulance Data Set (ADS).

If a patient is transferred from ambulance services to the care of an Emergency Department, information within the Ambulance Data Set is subsequently linked with key information collected in Emergency Departments as part of the Emergency Care Data Set (ECDS).

The purpose of this is to fully understand the patient's journey from the ambulance service to other urgent and emergency healthcare settings. This will enable clinicians, ambulance services and the NHS to learn from patient journeys and further improve the care they provide in the future.

Data collected by ambulance services and emergency departments is securely linked and transferred to us. Data collected as part of the Ambulance Data Set is shared with NHS Digital* – a section of NHS England specialised in data and IT systems – where it is linked with key relevant information in the Emergency Care Data Set and securely returned to us.

This linked information includes a unique number generated by us during the initial 999 call, as well as a unique vehicle reference which will help us re-identify the original care record for the incident and the patient.

Appropriate access to this information will enable us to help develop the skills of our clinicians to improve the care they provide and support us in delivering service improvements to improve patient experience.

Patients will be able to opt out from this process if they so wish and data about their emergency care will remain with the ambulance service and / or the Emergency Department. To opt out of this process, please see the section entitled National data opt-out below.

For more information about the National Data Opt-Out, please visit

National Data Opt-Out - NHS England Digital

The lawful basis for the ambulance service to process this information under UK General Data Protection Regulation (UK GDPR) is Article 6 (1)(e) – "…exercise of official authority" and for processing special categories (health) data the basis is: Article 9(2)(h) – '…health or social care…' of the UK GDPR Regulations.

For the data collected by ambulance services (ADS) to be linked with relevant data items collected at Emergency Departments (ECDS) the lawful basis is the Sections 254(1), (3), (5) and (6), section 260(2)(d), section 261(2)(e) and section 304(9), (10) and (12) of the Health and Social Care Act 2012, as per the Ambulance Data Set

To lawfully process information in the manner described, NHS England on behalf of ambulance services have obtained a section 251 approval, as required by the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002. This provides a legal basis for patient information to be processed for these purposes.

NHS Digital officially merged with NHS England on 1st Feb 2023, therefore the organisation previously known as NHS Digital is legally known as NHS England and data held by NHS Digital is now held within NHS England.

Information Shared with the Infected Blood Compensation Authority (IBCA)

If you have made a claim for compensation through the Infected Blood Compensation Authority (IBCA), London Ambulance Service NHS Trust may provide IBCA with relevant information from your medical records to support your claim. You can read more about how IBCA uses your information in their privacy notice (available at: https://ibca.org.uk/privacy).

National data opt-out

We are applying the national data opt-out because we are using confidential patient information for planning or research purposes

The information collected about you when you use health and care services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear lawful basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential health and care information is only used like this when allowed by law.

Whenever possible data used for research and planning is anonymised, so that you cannot be identified and your confidential information is not accessed.

You have a choice about whether you want your confidential information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit National Data Opt-Out - NHS England Digital

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

Is information transferred outside the UK?

Your information may be processed in a third country because the relevant servers are located there. Any data processed in a third country will only be approved following the completion of a Data Protection Impact Assessment, a Digital Impact Assessment, a Third Party Supplier Questionnaire and will also be subject to UK GDPR regulations regarding the processing of data in a third country.

Information relating to your health and wellbeing and other special category data

We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees.

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e. Statement of Fitness for Work from your GP or hospital.
- Accident records if you have an accident at work.
- Information provided with consent to match appropriate alternative duties hub placements.
- Details of any desk audits, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, gender identification and may be extended to include other protected characteristics.

What is our lawful basis for using information?

Personal information

In order for the sharing of data to comply with Article 5 of the UK General Data Protection Regulation (UK GDPR) it must be fair and lawful, and one of the Article 6 conditions must be met. An article 9 condition must also be met if sensitive personal data or special category data is being shared.

Depending upon the processing activity, the lawful basis we rely on for using personal information are:

- Article 6(1)(a) which relates to the processing where consent has been freely given.
- Article 6(1)(b) which relates to processing necessary for the performance of a contract.
- Article 6(1)(c) so we can comply with our legal obligations as your employer.
- Article 6(1)(d) in order to protect your vital interests or those of another person.
- Article 6(1)(e) for the for the performance of our public task.
- Article 6(1)(f) for the purposes of our legitimate interest.

More sensitive data

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

- Article 9(2)(a) which relates to explicit consent freely given
- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights in law
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent
- Article 9(2)(f) for the establishment, exercise or defence of legal claims
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee or within the remits of your association to the Trust
- Article 9(2)(j) for archiving, research and statistics in the public interest

In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) of the Data Protection Act (DPA) 2018.

These relate to the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee. Our Safeguarding Policy provides further information about this processing.

Criminal convictions and offences

We process information about staff criminal convictions and offences. The lawful basis we rely to process this data are:

- Article 6(1)(e) for the performance of our public task. In addition, we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a). Article 6(1)(b) for the performance of a contract. In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1.

Common Law Duty of Confidentiality

Common law, is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by Judges.

The general position is that if information is given in circumstances, where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. However, if a duty of confidence applies and its within the 'reasonable expectations' of an employee, or any others working within the Trust, that information will be shared, then this is not a breach of common law.

Information will be shared to ensure the Trust complies with all legal obligations, for the provision of good management and the delivery of best care. For full details of the justifiable exemptions for breaching confidentiality, please see the main Trust Privacy Notice Privacy Notice - London Ambulance Service NHS Trust

Data Sharing

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors. For example, we may share information about you with HMRC, for the purpose of collecting tax and national insurance contributions.

Additionally we are required under the Public Records Act 1958 (as amended) to transfer records to the National Archives (TNA) for permanent preservation. Some of these records may include the personal data of our current and former employees.

Full consideration will be given to Data Protection and Freedom of Information legislation, when making decisions about whether such records should be open to the public.

Please note, anonymised or redacted information shall be shared to third parties, such as, but not limited to, research bodies and media outlets. To ensure anonymity and possibilities of re-identification, the London Ambulance Service NHS Trust undertakes relevant appropriate privacy and security assessments before any disclosure.

How do you know your records will be kept confidential?

All NHS organisations have a legal duty of confidence to their patients, staff and those working with the organisation; as previously specified. The Data Protection legislation further defines how we can collect and handle personal information. The NHS also has an additional set of guidelines, known as the Caldicott Principles, which apply to the use of confidential information. All NHS organisations are required to appoint a Caldicott Guardian to ensure confidential information is handled in accordance with legal and NHS regulations and the Caldicott Guardian for the London Ambulance Service is the Medical Director.

When we pass on any information we will ensure that the recipient is aware that it must be kept confidential and secure.

How do we store your personal information?

Information is held for specified periods of time as set out in the Trust's Records Management and Information Lifecycle policy which accords with NHSX Records Management Code of Practice

We retain medical records for 25 years including clinical details obtained via 999 and 111 calls made by adults. Other records that may contain information about you are kept for varying lengths of time.

Records containing confidential information are destroyed in accordance with the Trust's Waste Management policy, paper records (including photographs, film, fiche and disks) being shredded, computer equipment having their drives security wiped, electronic devices having all data deleted and set to factory default, USB's having all drives security wiped, magnetic media data cartridges/cassettes having magnetic degaussing.

Your Rights over Your Information

Your right of access - You have the right to ask us for copies of your personal information we hold about you, please click on this link: **https://www.londonambulance.nhs.uk/talking-with-us/making-requests-for-the-records-we-hold/**
For further details regarding Subject Access Requests, please click this link which connects you to the NHS England website: subject access request.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. If you wish to contact about your records in this respect please do so at: londamb.staffsubjectaccessrequests@nhs.net
For further details regarding your rights to rectification, please click this link which connects you to the NHS England website: rectify personal information.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances. In general medical records can be corrected but have to be maintained.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information such as direct marketing or automated in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at if you wish to make a request at londamb.staffsubjectaccessrequests@nhs.net

Further Information

HR Personal files

Electronic records are securely held for each member of staff. Some data is held securely on LAS systems and at our premises and some data is held securely with our off site storage contractor Oasis Group.

You can request your personnel file by emailing our People & Culture Team on the following email address: londamb.staffsubjectaccessrequests@nhs.net

Personnel files are kept for 6 years after the date of leaving the trust.

Cycle and Car salary sacrifice schemes

These schemes allow you the use of a car or bicycle in exchange for a fixed monthly reduction from your gross salary taken before tax*, National Insurance and pension.

Your Car Benefit Scheme is managed by CPC Drive in partnership with Tusker, a recognised NHS car provider and is the smarter way to run a car. A fixed monthly amount is taken directly from your gross salary meaning you can save on National Insurance, and in return you get the use of a brand-new car – and Tusker sort everything else out at no extra cost.

The cycle scheme is run by Cycle Solutions – a popular scheme – you must order through the site and there is a £3k limit.

We have a 'White Goods' scheme too, which is also salary sacrifice – but that ranges from all sorts of tech, to sofas and boilers too. That is run by Liaison One Call and this is their link. This was seasonal, but is now open all year round.

Annual NHS Staff Survey (NSS)

The NHS Staff Survey runs annually. The survey is administered on behalf of the London Ambulance Service by the Picker Institute Europe, a charity independent of the NHS.

You will receive invitation and reminder emails via your NHS.net email address from Picker. This email will contain a unique link to complete the survey (you can do this via any computer, smart phone or tablet). All responses to this survey are strictly confidential and Picker will not share any identifiable information with the London Ambulance Service. The unique link is used so Picker can show our results at a team/station level, but to protect confidentiality, the London Ambulance Service will only receive results if 11 or more colleagues in a team respond to a survey.

If you need any help with completing your survey please email: londamb.survey@nhs.net

Any data collected by Picker for us is stored on UK servers. A link to their privacy notice can be found here https://picker.org/privacy-notice-for-online-surveys/

Most survey questions require quantitative responses, however some free text boxes are included. We would advise you not to share identifiable information about yourself in these boxes, if you wish to remain anonymous.

National Quarterly Pulse Survey (NQPS)

National Quarterly Pulse Survey is a short survey which allows colleagues to feed back their views to the organisation every quarter. It runs during the months of January, April and July, with the annual NHS Staff Survey running in the autumn.

We use the People Pulse tool provided by Ipsos Karian and Box to administer the NQPS on our behalf. Unlike the annual NHS Staff Survey, there is a universal link to access the survey: https://www.nhspeoplepulse.com/ and respondents need to select the Trust and group station/department they belong to. To protect confidentiality, the London Ambulance Service will only receive results at the department level if 11 or more colleagues respond to the survey.

Most survey questions require quantitative responses, however some free text boxes are included. We would advise you not to share identifiable information about yourself in these boxes if you wish to remain anonymous.

Any data collected by Ipsos Karian and Box is stored on servers within the Economic Area. A link to their privacy notice can be found here https://peoplepulse.qualtrics.com/ControlPanel/File.php?F=F_zKMo9RMAL75dnmd

Whistleblowers

The LAS has a policy and procedure in place to enable its current staff and ex-employees to have an avenue for raising concerns about malpractice.

If you wish to raise a concern please refer to ‘Speak up’ – The LAS’s whistleblowing policy and procedure.

Information in this context is processed by us because it is necessary for our compliance with our legal obligations under the Public Interest Disclosure Act 1998 and The Public Interest Disclosure (Northern Ireland) Order 1998.

Equal opportunities monitoring

Equal opportunities information provided by job applicants is attached to the relevant application on Health Jobs UK (TRAC Jobs) when you apply for a role at the London Ambulance Service.

This information is not made available to any staff outside our recruitment team (including hiring managers) in a way which can identify you. This information is anonymised and retained for reporting purposes only.

We are committed to promoting equal opportunities across everything we do, in terms of employment and training, providing services and our engagement and decision making. We welcome diversity and look for self-motivated, enthusiastic people from all backgrounds who care about making a difference.

We aim to:

- celebrate and encourage the diversity of our workforce
- create a working environment where everyone feels included and appreciated for their work
- promote and provide our training and employment opportunities without regard to age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation or any other aspect of a person’s background
- encourage creativeness and innovation, to ensure that each member of staff can give of their best and help us move forward with our equality and inclusion goals.

We have also joined Stonewall’s Health Champions programme, receiving free advice and expertise on health services from the charity.

Workforce Development and Planning

Our Workforce and Development and Planning department use online learning platforms such as Pulse for the facilitation of its work related courses. We also use the Education Governance Committee.

We will share some information about you with these providers both prior to you joining the LAS and during your employment to ensure you have the necessary access to complete training required for your role.

We will also share information about you with our training providers. For example this will include information such as your name, contact details and job role. When necessary we will also share information about any dietary or access requirements that you might have when you attend training events.

Occupational health

During your employment you may be referred to occupational health following a request to HR by you or your line manager. This may result in a face-to-face consultation, a telephone appointment with an occupational healthcare professional and/or a medical report from a GP or specialist. Please be aware that if you do not attend an appointment without cancelling the appointment or without leaving suitable notice of cancellation, your line manager may be informed.

In most cases the Trust uses Optima Health to provide our occupational health service. The information you provide will be held by Optima Health, who will give us a fit to work certificate or a report with recommendations. Pilot supporting absence projects are also in use within the Trust, for a small number of departments, to trial the success of an internal supporting absence service.

Trade Union Membership

The recognised union at the LAS (UNISON and GMB) are controllers for the personal information connected to your union membership. The LAS holds some UNISON and GMB union subscription details in order to process salary deductions for union membership for which staff will have given their consent.

Monitoring of staff

All of our ICT systems, EDRM system and the swipe access system for the entry and exit of our premises are auditable and can be monitored, though we don't do so routinely.

We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our ICT systems and equipment. However, we reserve the right to log and monitor such use in line with our Acceptable Use Standard.

Any targeted monitoring of staff will take place within the context of our disciplinary procedures.

Staff involved in criminal enforcement

If you are involved with the process of criminal enforcement – some staff in Legal, Intelligence or the Financial Recovery Unit – we monitor and log your access to the information being processed.

Part 3 of the Data Protection Act 2018, which concerns law enforcement processing requires us to keep logs. Section 62 states that these logs that make it possible to establish the identity of the person who consulted the data, the date and time it was consulted and the justification for doing so. Beyond this, the logs must make it

possible to establish the identity of the person disclosing the data, the date and time it occurred and the identity of the recipients. These logs will be kept to assist with self-monitoring by the LAS, including internal disciplinary proceedings, verifying the lawfulness of the processing, ensuring the integrity and security of personal data, and for the purposes of criminal or regulatory proceedings.

National Fraud Initiative (NFI) Privacy Notice

We are required by law to protect the public funds we administer. In order to prevent and detect fraud, we may share the information you provide with other organisations that audit or administer public funds. The Cabinet Office is responsible for carrying out data matching exercises.
Data matching involves comparing computer records held by one organisation with those held by the same or another organisation to identify the extent of any matches. These records usually contain personal information. Computerised data matching assists in identifying potentially fraudulent claims and payments. Where a match is identified, it may point to an inconsistency that needs further investigation. No conclusion can be drawn about whether this is fraud, error or another explanation until an investigation has taken place.
We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise that supports the prevention and detection of fraud – see guidance https://www.gov.uk/guidance/taking-part-in-national-fraud-initiative. We take privacy very seriously. Your data will always be handled securely and responsibly. Further details are available in the privacy notice guidance, which explains how your personal data will be used as part of the Cabinet Office's NFI data matching exercise to support fraud prevention and detection.
The Cabinet Office carries out data matching under statutory powers set out in Part 6 of the Local Audit and Accountability Act 2014. This processing is carried out under statutory powers and does not require the consent of individuals concerned under data protection legislation or the General Data Protection Regulation (GDPR).. For further details on why specific information is matched, see: Code of Data Matching Practice for the National Fraud Initiative - GOV.UK (www.gov.uk)
For further information on data matching at the Trust please contact Kirsty Clarke, Local Counter Fraud Specialist, by emailing kirsty.clarke@rsmuk.com. Further information on how the NFI has assisted the NHS and other public sector organisations can also be found at National Fraud Initiative case studies - GOV.UK (www.gov.uk)
Useful resources:
Right to be informed | ICO
A guide to the data protection exemptions | ICO
Getting copies of your information (SAR) | ICO
NFI Security Policy

Financial monitoring

We use a financial accounting system East Lancashire Financial Services (ELFS) to log every financial transaction. This includes any transactions or loans made by or to staff. If an outstanding debt by a member of staff is highlighted via this process, the LAS will use this information to take steps to recover the outstanding amount.

Security clearance

The Trust, in accordance with its legal obligations, seek DBS checks for all new staff where their job roles require them. Checks are sought prior to the staff member commencing work and as a condition of them doing so. Checks are also sought on a change of role into a post which requires a DBS check.

The Disclosure and Barring Service is a national service that provides a certificate upon request, containing information about a given individual's criminal record (should they have one) and their presence on any of the registered offenders lists or barred lists; that is to say if the individual is, for example, barred from working with children. An enhanced DBS additionally provides information about spent convictions and any intelligence short of a conviction that any authority holds on that individual; these are used for individuals with the potential to be working with children or vulnerable groups.

At the Trust, the majority of checks are carried out at an enhanced level with barring on the basis that our operational staff (including EOC and 111) could work with children or vulnerable groups. There are also a small number of standard and basic checks. The outcome of these checks are stored on our systems.

Security passes

All staff are all issued with a London Ambulance Service identification badge that displays their name, department, staff reference number and photograph. Staff pass details (names, numbers and photographs) are held on a standalone machine controlled by Estates and can only be accessed by a restricted number of people.

Photographs are uploaded by Estates staff. Should you lose your pass you will need to complete a lost security pass form and return it to Estates. When you leave the LAS your details are deleted as soon as possible from this system.

CCTV

We operate CCTV inside our premises at all LAS offices and stations to monitor access to certain areas. Further information is available in our CCTV policy.

Additionally, staff may be filmed by CCTV which is owned and operated by the landlords or owners of the buildings we use. The LAS is not the data controller for this information.

Disclosures under the Freedom of Information Act (2000)

As a public authority we receive information requests under the Freedom of Information Act (2000) about our staff and we must consider whether to disclose staff information (including agency and temporary staff) in response to these requests.

We will normally disclose work-related information about staff in a public-facing role. We may also disclose information about staff members whose work is purely administrative if their names are routinely sent out externally.

It is less likely that information about those who do not deal directly with the public in an operational capacity will be disclosed. The CEO Executive Team and the COO Executive Team will have more information disclosed about them, such as photographs and biographical detail, due to their position at the LAS.

We will consider withholding information if we think that it will prejudice our regulatory role or the rights and safety of our staff, irrespective of grade or position.

The type of information you can expect we will disclose is as follows:

- Name and work contact details.
- Pay bands (not your exact salary).
- How long you have worked at the LAS, your current role, any previous roles or secondments and what your role involves.
- Your position in the corporate structure.
- Business related entries in your diary/calendar.
- Summaries of expense claims without details of where you stayed, where you ate or your itinerary.
- Any work related training at the LAS.
- Any work related opinions, for example case notes containing your opinion about an investigation or a complainant

When we are asked to disclose diary or calendar information due consideration will be given to the safety of our staff. Where this information is requested outside of an FOI request our staff are advised to consult with their manager before sharing information about a staff member, especially when it concerns movements or whereabouts.

We will consult with you prior to deciding whether to disclose any information that we consider would not be within your reasonable expectations.

Before you begin working at the LAS, contact HR if you need to make us aware of a specific reason why your information cannot be provided as part of a disclosure. At any later point, if you have any concerns about information being released you need to inform us of this fact.

Requests for references

If you leave, or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference, if you have provided them with our details. For example we may be asked to confirm the dates of your employment, your job role, absence relating to sickness and any current formal sanctions

How do I complain?

You have the right to raise a concern if you think the Trust is processing your personal data incorrectly. Please contact your line manager in the first instance.

If you require further information about how we process your personal data, you may also contact the Information Governance team at lonamb.informationgovernance@nhs.net

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

Date of last review

20th October 2026 - next review 1st December 2026