

Employee Privacy Notice

This Privacy Notice explains how LILA Liverpool Limited collects, uses, stores and protects personal data relating to employees, workers, contractors and applicants in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

What information we collect and process

We may collect, store and process the following categories of personal data:

1. Personal and contact details including your name, address, telephone number, email address, date of birth and emergency contact details.
2. Employment information including your job title, role, salary, benefits, contractual terms, working hours and employment history.
3. Financial information including bank account details, National Insurance number, tax information, pension information, payroll records and payslips.
4. Right to work documentation including passport information, visa documentation and immigration status checks.
5. Qualifications and professional information including references, CVs, interview notes, training records, licences, certificates and professional memberships.
6. Performance and conduct information including appraisals, supervision notes, attendance records, disciplinary, grievance and capability records.
7. Health and wellbeing information including sickness absence records, occupational health information, fitness for work assessments and reasonable adjustment requirements where applicable.
8. Equality and diversity information including protected characteristic data for monitoring and compliance purposes.
9. Safeguarding and safer recruitment information including DBS checks, Online checks, criminal convictions information where lawfully required, safeguarding concerns and safeguarding training records.
10. IT and security information including usernames, log-in details, email usage, internet usage, device usage and access logs.
11. CCTV images and building access records where applicable for safeguarding, health and safety, security and crime prevention purposes.
12. Communications and correspondence including emails, letters, meeting notes and records of communications between you and the organisation.

Why we hold and process information about you

- Recruitment and safer recruitment checks
- Managing your employment and contractual relationship
- Payroll, pensions and benefits administration
- Compliance with legal and regulatory obligations
- Safeguarding children, young people and vulnerable adults
- Monitoring attendance, performance and conduct
- Managing health, safety and wellbeing
- Training and professional development
- Protecting organisational systems, property and information

- Investigating complaints, disciplinary matters or safeguarding concerns
- Defending or pursuing legal claims where necessary

Lawful bases for processing

We process your personal data under one or more of the following lawful bases:

- Performance of a contract
- Compliance with a legal obligation
- Legitimate interests pursued by the organisation
- Employment, social security and social protection law obligations
- Protection of vital interests
- Explicit consent where required

Where special category data is processed, including health, equality, safeguarding or criminal records data, this will only be processed where there is an appropriate lawful basis under UK GDPR and Schedule 1 of the Data Protection Act 2018.

Monitoring and IT usage

To protect our systems, employees, students and business operations, we may monitor the use of organisational IT systems, email accounts, internet usage, communication systems and devices where lawful and proportionate to do so. Monitoring may take place for safeguarding, cybersecurity, operational, investigative or compliance purposes.

Employees should have no expectation of complete privacy when using organisational systems for work purposes.

How we protect your information

We take appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, disclosure or destruction. These measures include:

- Restricted access controls
- Password protection and secure authentication
- Secure electronic and physical storage
- Staff training on confidentiality and data protection
- Security monitoring and regular system reviews
- Data breach reporting and response procedures

Data Breaches

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify affected individuals and the relevant supervisory authority where required by law

Who is responsible for protecting your information

The person responsible for the protection of your data is:

Senior Leadership Team

What your information will be used for

Your data will be used to assign you work, provide you with hours of work, pay you, monitor your performance, write to you with important documents, check your skills, qualifications and experience, appraise your performance and safeguard your health, safety and wellbeing in the workplace.

This is done on the basis of your being a party to a contract of employment and in the legitimate interests to safeguard your health, safety and welfare and the health, safety and welfare of your colleagues, clients and third parties in the workplace. The failure to provide us with the data may impact upon your recruitment, employment or tasks, duties and responsibilities with your role and/or assignment. You should discuss the further impact of this with your manager.

Who we share your information with

We may share personal data where necessary with:

- HM Revenue & Customs (HMRC)
- Pension providers and pension regulators
- Payroll providers
- Occupational health providers
- Legal and professional advisers
- Insurers and auditors
- IT support and cloud service providers
- Safeguarding agencies and statutory authorities where required
- Courts, tribunals and regulators
- Accrediting and inspection bodies where required

We will only share information where there is a lawful basis to do so and where appropriate safeguards are in place.

International transfers

Where personal data is transferred outside the United Kingdom, we will ensure that appropriate safeguards are in place in accordance with UK GDPR requirements.

How long we keep your information

Employment records will generally be retained for the duration of employment and for up to 6 years following the end of employment unless a longer retention period is required by law, safeguarding obligations or ongoing legal proceedings.

Certain records, including safeguarding information, immigration records and pension or tax documentation, may be retained for longer where required by legislation or regulatory guidance.

DBS information will only be retained for as long as legally permitted and necessary for safeguarding and recruitment purposes.

Your rights

Under UK GDPR you have the right to:

- Be informed about how your data is used
- Request access to the personal data we hold about you
- Request correction of inaccurate or incomplete data
- Request erasure of data in certain circumstances
- Request restriction of processing
- Object to processing where applicable
- Request transfer of your data to another organisation where applicable
- Withdraw consent where processing is based on consent
- Challenge automated decision making where applicable

Requests should be made in writing to the contact listed above.

Complaints

If you have concerns about how your data is handled, we encourage you to raise these with us in the first instance.

You also have the right to lodge a complaint with the [Information Commissioner's Office \(ICO\)](#).

Version History

Review Date	Review by	Review Reason & Notes
30/05/2018	Katherine Watson	Initial document. GDPR compliance. Based upon ELAS document SEC-024b, version 1 (17/04/2018) "Employee Privacy Notice (without consent)".
29/11/2021	Simone Amaglio	Annual Review
2023	Victoria Bligh	Annual Review
2024	Stacey McGee	Annual Review
2026	Victoria Bligh	Annual Review