

LEO™ PRIVACY POLICY

LEO HR LTD

Company Number: **17324775**

ICO Registration Number: **ZC191813**

Website: www.leohr.co.uk

Email: **office@leohr.co.uk**

Jurisdiction: **England & Wales**

Document Control

Item	Details
Document	LEO™ Privacy Policy
Version	2.0
Status	Controlled Master Document
Owner	LEO HR LTD
Effective Date	7 th July 2026
Review Frequency	Annual or following any material legal, regulatory or Platform change
Classification	Public
Jurisdiction	England & Wales

Copyright

© 2026 LEO HR LTD. All rights reserved.

LEO™, Ask LEO™, LEO Talent™, LEO Learn™, AI Studio™, Foundations™, Connections™ and all associated branding, software, documentation, workflows and proprietary methodologies are the intellectual property of LEO HR LTD unless otherwise stated.

This Privacy Policy forms part of the LEO™ Legal & Governance Framework and should be read alongside our:

- Platform Terms & Conditions
- Cookie Policy
- Data Processing Agreement
- Acceptable Use Policy
- AI Transparency & Responsible Use Policy
- Information Security Policy
- Data Retention & Deletion Policy
- Trust Centre

1. Introduction

LEO HR LTD ("**LEO™**", "**we**", "**our**" or "**us**") is committed to protecting the privacy, confidentiality and security of the personal data entrusted to us.

LEO™ is an employment operating platform designed for organisations in England and Wales. The Platform enables employers to manage employment relationships, recruitment, learning, compliance and organisational knowledge while supporting informed workplace decision-making through artificial intelligence and workflow automation.

We recognise that the Platform may contain sensitive employment information, special category personal data and confidential organisational information. Protecting that information is fundamental to the design, operation and ongoing development of LEO™.

This Privacy Policy explains:

- what personal data we collect;
- why we collect it;
- how we use it;
- the lawful bases on which we process it;
- who we may share it with;
- how we protect it;
- how long we retain it; and
- the rights available to individuals under applicable data protection legislation.

2. Scope of this Privacy Policy

This Privacy Policy applies whenever personal data is processed by LEO HR LTD in connection with:

- the LEO™ website;
- customer accounts;
- subscriptions;
- the LEO™ Platform;
- Dashboard;
- Ask LEO™;
- Matters;
- Employees;
- Compliance;
- HR Resources;
- LEO Talent™;
- LEO Learn™;
- AI Studio™;
- Foundations™;
- Connections;
- SAR Requests;
- Insights;
- Audit Logs;
- Welcome Brief;
- Organisation;
- customer support services;
- billing and account administration; and
- any other services provided by LEO HR LTD.

This Policy also applies to personal data processed before, during and after a Customer's subscription where processing is required for legal, contractual or legitimate business purposes.

3. Definitions

For the purposes of this Privacy Policy:

Authorised User means any individual authorised by a Customer to access the Platform.

Customer means the organisation that has entered into an agreement with LEO HR LTD for the provision of Platform Services.

Customer Data means all information uploaded, entered, created or generated by a Customer when using the Platform.

Data Controller has the meaning given by UK GDPR.

Data Processor has the meaning given by UK GDPR.

Organisation Knowledge means organisation-specific information stored within Foundations™, uploaded documentation and other authorised Platform content that enables LEO™ to provide organisation-specific assistance.

Personal Data means any information relating to an identified or identifiable natural person.

Platform means the LEO™ software platform and its associated services.

Platform Data means operational information automatically generated by the Platform, including audit logs, authentication events, workflow activity, usage information and security records.

Processing has the meaning given by UK GDPR and includes collecting, recording, storing, organising, retrieving, analysing, using, sharing, archiving and deleting personal data.

Special Category Data means personal data requiring additional protection under Article 9 of UK GDPR, including information relating to health, disability, trade union membership and other protected categories.

4. Our Privacy Principles

Privacy is embedded throughout the design and operation of LEO™.

When processing personal data, LEO HR LTD is committed to:

- processing personal data lawfully, fairly and transparently;
- collecting only information that is necessary for the purposes identified;
- ensuring personal data is accurate and kept up to date where appropriate;

- protecting personal data through appropriate technical and organisational measures;
- restricting access to authorised users on a need-to-know basis;
- supporting Customers in meeting their own data protection obligations;
- embedding security and privacy into the development of the Platform; and
- regularly reviewing and improving our privacy and security practices.

These principles underpin the design and operation of every LEO™ service.

5. Data Protection Legislation

LEO HR LTD processes personal data in accordance with applicable legislation, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where applicable; and
- guidance published by the Information Commissioner's Office (ICO).

Our ICO Registration Number is: **ZC191813**

6. Data Protection Roles

Depending upon the nature of the processing, LEO HR LTD may act as either a **Data Controller** or a **Data Processor**.

6.1 Where We Act as a Data Processor

In most cases, where Customers upload employment records or other organisational information to LEO™, they determine why and how that information is processed.

In these circumstances:

- the Customer is the **Data Controller**; and
- LEO HR LTD acts as the **Data Processor**, processing personal data only on the Customer's documented instructions unless otherwise required by law.

This includes, for example, information processed within:

- Employees;
- Matters;
- LEO Talent™;
- LEO Learn™;
- AI Studio™;
- Foundations™;
- SAR Requests; and
- other customer-managed Platform modules.

6.2 Where We Act as a Data Controller

LEO HR LTD acts as an independent **Data Controller** where we determine the purposes and means of processing personal data relating to our own business operations.

This includes processing relating to:

- customer account creation;
- subscription management;
- billing and payment administration;
- customer communications;
- technical support;
- platform security;
- fraud prevention;
- legal and regulatory compliance;
- recruitment by LEO HR LTD; and
- operation of our website and business.

6.3 Joint Responsibility

There may be limited circumstances where LEO HR LTD and a Customer each have separate legal responsibilities for different aspects of the same processing activity.

Nothing in this Privacy Policy alters the responsibilities placed on either party by applicable data protection legislation.

Customers remain responsible for ensuring they have an appropriate lawful basis for collecting and processing personal data within the Platform.

7. Categories of Personal Data We Process

The personal data processed by LEO™ depends on the services used by each Customer.

Not every Customer will use every module, and not every category of information listed below will be processed by every organisation.

7.1 Account Information

To create and manage customer accounts, we may process:

- name;
- business name;
- company registration number;
- email address;
- telephone number;
- job title;
- postal address;
- subscription information;
- billing information;
- payment status;
- communication preferences;
- authentication credentials;
- multi-factor authentication information;
- user permissions;
- account settings; and
- customer support history.

7.2 Organisation Information

Customers may choose to store information relating to their organisation, including:

- organisation profile;
- departments;
- business locations;
- management structures;
- working patterns;
- payroll cycles;
- holiday years;
- organisational policies;
- operational procedures;
- compliance frameworks;
- organisational knowledge stored within Foundations™;
- company documents;
- custom settings; and
- other organisation-specific information entered by authorised users.

7.3 Employee Information

Where the Employees module is used, Customers may process personal data relating to employees, workers, contractors, volunteers or agency workers.

This may include:

- identification details;
- contact information;
- emergency contacts;
- employment information;
- payroll identifiers;
- National Insurance number;
- contractual information;

- salary and benefits;
- working hours;
- absence records;
- holiday records;
- probation records;
- performance information;
- disciplinary records;
- grievance records;
- investigation records;
- capability records;
- consultation records;
- flexible working records;
- learning records;
- qualifications;
- professional registrations;
- right to work documentation;
- DBS and safeguarding records;
- driving information;
- medical information;
- occupational health information;
- uploaded employment documents; and
- employment history maintained within the Platform.

Some of this information may constitute **special category personal data** or **criminal offence data** under UK GDPR.

7.4 Recruitment Information

Where LEO Talent™ is used, Customers may process information relating to applicants and prospective employees, including:

- application details;
- CVs;
- application forms;
- interview records;
- assessment outcomes;
- references;
- qualifications;
- right to work documentation;
- recruitment communications;
- offer documentation;
- due diligence records;
- onboarding information; and
- recruitment workflow activity.

Where an applicant becomes an employee, relevant recruitment information may be transferred into the employee record to support continuity throughout the employment lifecycle.

7.5 Learning and Development Information

Where LEO Learn™ or AI Studio™ is used, Customers may process information relating to workplace learning and professional development, including:

- assigned learning;
- learning pathways;
- completed courses;
- certificates;
- qualifications;
- assessment results;

- competency records;
- CPD history;
- mandatory training;
- optional learning;
- development plans;
- manager feedback; and
- AI-assisted learning content generated within the Platform.

7.6 Employment Matters

Where Matters is used, Customers may process information relating to workplace issues and case management, including:

- matter titles;
- matter categories;
- chronology entries;
- employee involvement;
- investigation information;
- witness information;
- meeting records;
- correspondence;
- uploaded evidence;
- generated documents;
- recommendations;
- actions;
- workflow history;
- decisions;
- outcomes; and
- archived matter records.

7.7 AI Interactions

Where Ask LEO™, AI Studio™ or other AI-powered services are used, the Platform may process:

- prompts submitted by authorised users;
- questions;
- uploaded documents;
- organisational knowledge;
- generated responses;
- generated workplace documents;
- summaries;
- recommendations;
- action plans;
- learning content;
- workflow suggestions;
- compliance guidance; and
- analytical insights.

AI interactions are processed solely to provide the functionality requested by the Customer.

Customer information is **not** intentionally shared between organisations.

Unless expressly stated otherwise, Customer personal data is **not** used to train publicly available artificial intelligence models.

7.8 Foundations™ and Organisation Knowledge

Customers may build organisation-specific knowledge within Foundations™ to enable LEO™ to provide more relevant assistance.

This information may include:

- organisational structures;
- employment frameworks;
- policies;

- procedures;
- templates;
- guidance;
- historical matters;
- uploaded documentation;
- organisational preferences; and
- other information intentionally added by authorised users.

Organisation Knowledge remains logically separated from other Customers and is only used to provide services to the organisation that created it.

7.9 Connections

Where Customers choose to connect authorised third-party services through Connections, LEO™ may process information exchanged between the Platform and those connected services in accordance with the permissions granted by the Customer.

The categories of information exchanged will depend on the services connected and the functionality enabled.

LEO HR LTD processes such information only to facilitate the requested integration and does not control how independent third-party providers process information once it has been received by them.

7.10 Platform and Technical Information

To operate the Platform securely and efficiently, LEO™ automatically generates technical and operational information, including:

- login activity;
- authentication records;
- audit logs;
- user permissions;
- workflow activity;
- document creation and modification events;
- security events;

- device information;
- browser information;
- operating system;
- IP address;
- session identifiers;
- diagnostic information;
- feature usage;
- performance metrics; and
- error logs.

This information is primarily used for security, troubleshooting, service improvement and regulatory compliance.

7.11 Customer Support Information

Where Customers contact LEO HR LTD, we may process information including:

- support requests;
- email correspondence;
- telephone notes;
- live chat communications;
- uploaded files;
- screenshots;
- diagnostic information;
- troubleshooting records; and
- customer feedback.

8. How We Use Personal Data

LEO HR LTD processes personal data only where there is an appropriate lawful basis under UK GDPR.

Depending on the circumstances, personal data may be used to:

- provide the LEO™ Platform and associated services;
- create and manage customer accounts;
- authenticate authorised users;
- administer subscriptions;
- process payments;
- provide customer support;
- maintain organisation records;
- manage recruitment;
- support onboarding;
- manage employment throughout the employee lifecycle;
- deliver learning and development services;
- generate workplace documentation;
- support AI-assisted functionality;
- maintain audit records;
- improve Platform performance;
- monitor service availability;
- protect Platform security;
- investigate suspected misuse;
- comply with legal obligations;
- establish, exercise or defend legal claims; and
- communicate with Customers regarding the Platform.

We will only process personal data for purposes that are compatible with those for which it was originally collected or where otherwise permitted by law.

9. Lawful Bases for Processing

Depending on the circumstances, LEO HR LTD relies upon one or more of the following lawful bases under UK GDPR:

Lawful Basis	Typical Examples
Performance of a Contract	Providing the Platform, managing subscriptions, delivering services
Legal Obligation	Taxation, regulatory compliance, responding to lawful requests
Legitimate Interests	Platform security, fraud prevention, service improvement, business administration
Consent	Optional cookies, marketing communications and other processing where consent is required
Establishment, Exercise or Defence of Legal Claims	Managing disputes and protecting legal rights

Where consent is relied upon, it may be withdrawn at any time. Withdrawal of consent does not affect processing carried out before consent was withdrawn.

10. Artificial Intelligence and Personal Data

10.1 Responsible Use of Artificial Intelligence

Artificial intelligence is an integral part of LEO™ and supports many of the Platform's services, including Ask LEO™, AI Studio™, LEO Learn™, LEO Talent™ and other AI-assisted functionality.

Our approach to AI is based on the principle that technology should support informed workplace decision-making rather than replace human judgement.

AI is used to assist authorised users by:

- answering employment-related questions;
- analysing workplace scenarios;
- generating workplace documentation;
- organising organisational knowledge;
- producing summaries;

- assisting with recruitment;
- supporting learning and development;
- identifying potential compliance considerations;
- suggesting practical next steps; and
- improving productivity across the Platform.

Employment decisions remain the responsibility of the Customer.

10.2 How AI Processes Information

Where an authorised user chooses to use AI-powered functionality, LEO™ may process information submitted to the Platform in order to provide the requested service.

Depending upon the feature being used, this may include:

- prompts submitted by users;
- uploaded documents;
- employee information;
- recruitment information;
- organisational knowledge;
- workplace records;
- historical matters;
- policies and procedures;
- learning information; and
- other information intentionally supplied by authorised users.

Information is processed only to provide the requested functionality and is not processed for unrelated purposes.

10.3 Organisation Knowledge

Where Customers build Organisation Knowledge within Foundations™ or other authorised Platform modules, that information may be used to provide responses that better reflect the Customer's own organisation.

Organisation Knowledge remains isolated to the Customer organisation that created it.

Information from one Customer is not intentionally used to provide responses to another Customer.

10.4 AI-Generated Content

AI-powered services may generate:

- letters;
- reports;
- policies;
- procedures;
- meeting notes;
- investigation documentation;
- disciplinary documentation;
- grievance documentation;
- learning content;
- assessments;
- certificates;
- summaries;
- chronologies;
- action plans;
- recruitment documentation;
- compliance guidance; and
- other workplace documentation requested by authorised users.

Generated content is based upon the information available at the time it is created.

Customers remain responsible for reviewing all AI-generated outputs before relying upon or implementing them.

10.5 AI Privacy Commitments

LEO HR LTD is committed to the responsible processing of personal data through AI.

Accordingly:

- Customer information is processed only to deliver the requested Platform functionality.
- Organisation Knowledge remains logically separated between Customers.
- Personal data is processed only where reasonably necessary.
- AI processing is subject to role-based permissions and security controls.
- We seek to minimise the personal data processed wherever reasonably practicable.
- We regularly review AI functionality to ensure it continues to operate responsibly and lawfully.

10.6 Public AI Model Training

LEO HR LTD does **not** use Customer personal data, Organisation Knowledge or uploaded employment documentation to train publicly available artificial intelligence models.

Where trusted third-party AI providers are used to deliver Platform functionality, information is processed solely for the purpose of providing the requested service and subject to appropriate contractual, technical and organisational safeguards.

Further information about AI governance is available within the **AI Transparency & Responsible Use Policy** and the **LEO™ Trust Centre**.

10.7 Human Oversight

LEO™ does not make employment decisions on behalf of Customers.

Customers remain responsible for:

- reviewing AI-generated content;
- verifying factual accuracy;
- considering the circumstances of each workplace situation;
- ensuring compliance with applicable legislation; and

- exercising appropriate professional judgement.

AI assists decision-making but does not replace human responsibility.

11. Sharing Personal Data

11.1 Our Approach

LEO HR LTD does not sell personal data.

We do not trade Customer information or permit third parties to use Customer personal data for their own marketing purposes.

Personal data is shared only where necessary to:

- provide the Platform;
- fulfil contractual obligations;
- comply with legal requirements;
- maintain Platform security;
- support Customers; or
- facilitate authorised integrations.

11.2 Categories of Recipients

Depending on the services used, personal data may be shared with trusted service providers supporting:

- cloud infrastructure;
- secure databases;
- authentication;
- payment processing;
- email delivery;
- customer communications;
- artificial intelligence;
- customer support;
- analytics;
- disaster recovery;

- professional advisers;
- insurers; and
- regulators or law enforcement where legally required.

All service providers are selected with appropriate consideration for security, confidentiality and compliance with applicable data protection legislation.

Current sub-processors are identified within the **LEO™ Trust Centre**.

11.3 Third-Party Integrations

Where Customers choose to connect external systems using Connections, information may be exchanged between LEO™ and those authorised services in accordance with the permissions granted by the Customer.

Customers remain responsible for reviewing the privacy practices of any third-party services they choose to connect.

11.4 Legal Disclosure

LEO HR LTD may disclose personal data where required to:

- comply with applicable law;
- comply with court orders;
- comply with regulatory requirements;
- protect legal rights;
- investigate suspected unlawful activity;
- establish, exercise or defend legal claims; or
- protect the security or integrity of the Platform.

Any disclosure will be limited to the information reasonably necessary for the relevant purpose.

12. International Data Transfers

LEO HR LTD is committed to ensuring that personal data remains appropriately protected whenever it is transferred outside the United Kingdom.

Where international transfers occur, we will implement appropriate safeguards in accordance with UK GDPR.

These safeguards may include:

- UK International Data Transfer Agreements (IDTAs);
- the UK Addendum to the European Commission's Standard Contractual Clauses;
- adequacy regulations;
- contractual commitments;
- encryption;
- technical safeguards; and
- organisational safeguards.

Where Customers independently choose to connect third-party services through Connections, they remain responsible for ensuring those services are used lawfully.

13. Information Security

13.1 Security Principles

Protecting Customer information is fundamental to the operation of LEO™.

We implement technical and organisational measures designed to protect the confidentiality, integrity and availability of personal data.

Security controls are reviewed regularly and enhanced where appropriate.

13.2 Security Measures

Depending on the services used, security measures may include:

- encrypted communications;
- encrypted storage where appropriate;
- secure authentication;

- multi-factor authentication;
- role-based permissions;
- access controls;
- audit logging;
- secure backups;
- vulnerability management;
- infrastructure monitoring;
- disaster recovery arrangements;
- business continuity planning; and
- secure software development practices.

Security measures evolve over time to address emerging threats and changes in technology.

13.3 Customer Responsibilities

Customers remain responsible for:

- maintaining secure passwords;
- protecting authentication credentials;
- assigning appropriate permissions;
- promptly removing access for departing users;
- ensuring personal data entered into the Platform is processed lawfully; and
- maintaining appropriate internal security procedures.

13.4 Security Incidents

Where LEO HR LTD becomes aware of a security incident affecting Customer information, we will investigate promptly and take reasonable steps to:

- contain the incident;
- minimise any impact;
- restore affected services where practicable;
- notify affected Customers where legally required; and
- comply with applicable legal and regulatory obligations.

14. Data Retention

LEO HR LTD retains personal data only for as long as reasonably necessary to:

- provide the Platform;
- fulfil contractual obligations;
- comply with legal obligations;
- maintain security;
- resolve disputes;
- establish, exercise or defend legal claims;
- support business continuity; and
- meet regulatory requirements.

Retention periods vary according to the type of information processed and the legal obligations that apply.

Further information is available within the **LEO™ Data Retention & Deletion Policy**.

Following the end of a Customer's subscription, information may continue to be retained for a limited period where necessary for:

- legal compliance;
- secure backups;
- disaster recovery;
- contractual obligations; or
- legitimate business purposes.

Where information is no longer required, it will be securely deleted, anonymised or archived in accordance with applicable legislation and our retention policies.

15. Your Privacy Rights

Individuals whose personal data is processed by LEO HR LTD may have rights under UK GDPR, subject to the circumstances of the processing and the lawful basis relied upon.

These rights include the right to:

- be informed about how personal data is processed;
- request access to personal data;
- request correction of inaccurate or incomplete personal data;
- request erasure of personal data where applicable;
- request restriction of processing;
- object to certain processing activities;
- request the transfer of personal data where applicable;
- withdraw consent where processing is based on consent; and
- lodge a complaint with the Information Commissioner's Office (ICO).

The availability of individual rights depends upon the nature of the processing and the applicable legal basis.

15.1 Subject Access Requests

Individuals may request access to personal data held by LEO HR LTD.

Where LEO HR LTD acts as a **Data Processor** on behalf of a Customer, requests relating to Customer data will normally be referred to the relevant Customer, who acts as the **Data Controller**.

LEO™ includes functionality designed to assist Customers in responding to Subject Access Requests in accordance with applicable legislation.

15.2 Rectification

Individuals may request correction of inaccurate or incomplete personal data.

Where appropriate, authorised users may update information directly within the Platform.

LEO HR LTD will provide reasonable assistance to Customers where required and appropriate.

15.3 Erasure

Individuals may request deletion of personal data where permitted by law.

Requests will be considered in accordance with:

- UK GDPR;
- contractual obligations;
- legal retention requirements;
- regulatory obligations;
- the rights of other individuals; and
- LEO HR LTD's Data Retention & Deletion Policy.

Certain information cannot be deleted immediately where retention is required by law or is necessary to establish, exercise or defend legal claims.

15.4 Restriction of Processing

Individuals may request that processing of their personal data be restricted in circumstances provided for by UK GDPR.

During any period of restriction, personal data may continue to be stored but will not otherwise be processed except where permitted by law.

15.5 Objection

Individuals may object to processing carried out on the basis of legitimate interests.

Each objection will be considered individually, taking into account the legal rights and legitimate interests of all parties.

15.6 Data Portability

Where required by law, individuals may request a copy of certain personal data in a structured, commonly used and machine-readable format.

This right applies only where the legal conditions set out in UK GDPR are met.

15.7 Withdrawing Consent

Where processing is based upon consent, consent may be withdrawn at any time.

Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

16. Cookies and Similar Technologies

LEO™ uses cookies and similar technologies to support:

- secure authentication;
- user sessions;
- Platform functionality;
- security;
- accessibility;
- performance monitoring; and
- user preferences.

Where required by law, consent will be obtained before non-essential cookies are placed on a user's device.

Further information is available in the **LEO™ Cookie Policy**.

17. Changes to this Privacy Policy

LEO HR LTD may amend this Privacy Policy where reasonably necessary to reflect:

- changes in legislation;
- updated regulatory guidance;
- improvements to the Platform;
- new functionality;
- security enhancements;
- changes to our service providers;
- operational requirements; or
- improvements to our privacy practices.

Where changes materially affect how personal data is processed, we will take reasonable steps to notify Customers through one or more of the following:

- email;
- in-platform notification;
- publication on the LEO™ website; or
- publication within the LEO™ Trust Centre.

The latest version of this Privacy Policy will always be available through the LEO™ website and Platform.

18. Contact Us

If you have questions about this Privacy Policy or the way LEO HR LTD processes personal data, please contact:

LEO HR LTD

Company Number: **17324775**

ICO Registration Number: **ZC191813**

Website: www.leohr.co.uk

Email: **office@leohr.co.uk**

Jurisdiction: **England & Wales**

If you are dissatisfied with our response, you have the right to lodge a complaint with the **Information Commissioner's Office (ICO)**.

Schedule 1 – Related Documents

This Privacy Policy forms part of the wider **LEO™ Legal & Governance Framework** and should be read alongside:

- Platform Terms & Conditions
- Cookie Policy
- Data Processing Agreement
- Acceptable Use Policy
- AI Transparency & Responsible Use Policy

- Customer Support Policy
- Information Security Policy
- Data Retention & Deletion Policy
- Trust Centre

Schedule 2 – Data Protection Principles

LEO HR LTD processes personal data in accordance with the principles set out in UK GDPR.

Accordingly, personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where appropriate;
- retained only for as long as necessary;
- protected through appropriate technical and organisational measures; and
- processed in a manner that ensures appropriate security and confidentiality.

These principles underpin the design, operation and ongoing development of LEO™.

Schedule 3 – Document Version History

Version	Date	Summary
1.0	7 July 2026	Initial Privacy Policy
2.0	Launch Edition	Comprehensive rewrite aligned with the live LEO™ platform, Version 2.0 legal framework, UK GDPR, PECR and responsible AI governance. Updated Platform modules, clarified Controller/Processor roles, strengthened AI privacy commitments, introduced Trust Centre references and improved readability.

Final Statement

LEO HR LTD believes that privacy is fundamental to trusted workplace technology.

LEO™ has been designed with privacy, security and responsible artificial intelligence at its core, enabling organisations to manage employment information confidently while maintaining strong governance, transparency and compliance.

We are committed to continuously reviewing and improving our privacy practices to reflect developments in technology, legislation and regulatory guidance, ensuring that the Platform continues to meet the high standards expected by our Customers.