Meeting	OLC Board Meeting	**Agenda Item No**. **Paper No**.	3 138.2
Date of meeting	29 April 2025	**Time required**	30 Minutes

Title	LeO's strategic approach to digital technology and AI
Sponsor	David Peckham, Head of Operations, Business Intelligence, Operational Transformation, IT
Status	OFFICIAL
To be communicated to:	Members and those in attendance

Executive summary

In October 2024, LeO updated the OLC board on its digital technology and AI approach including what was being developed at that point and LeO's ambition to create a wider strategic approach to digital transformation and the governance framework that underpinned that. The board supported adopting digital transformation subject to several considerations to ensure that digital transformation and specifically AI were being implemented in a way that was secure, ethical, well-considered and complimented LeO's approach to achieving strategic aims for 2024-2027.

This paper covers LeO's approach, leveraging technology whilst addressing legitimate concerns, including:

- **Draft 2025-27 Digital Transformation Strategy**
  The strategy aims to leverage technology to support LeO's objectives, focusing on:
  1. Enhancing complaint resolution efficiency.
  2. Using data analytics for actionable insights.
  3. Integrating AI and automation to streamline processes and improve service accuracy.
- **Key Initiatives and Progress**
- **2025/26 Next Steps**
- **Additional Developments**

Recommendation / action required
Board members are asked to review and feedback on LeO's approach to digital transformation. Feedback is particularly sought on: • LeO's draft 2025-27 Digital Transformation Strategy • Views on LeO's approach to 2025/26 actions. • Broader views and experience of progress, risks and challenges elsewhere
Equality Diversity and Inclusion

EDI implications	**Yes**
Using AI brings many impacts and risks and could pose potential unknown risks in terms of LeO's delivery from an EDI perspective. AI has the potential to perpetuate bias if trained on bias data, leading to unfair outcomes. Lack of diversity in development could also result in discriminatory AI tools. Over-reliance on AI without human oversight can exacerbate bias. Data privacy concerns could also arise, particularly affecting marginalised communities.	
Freedom of Information Act 2000 (FoI)	
Paragraph reference	**FoI exemption and summary**
N/A	N/A

LeO’s strategic approach to digital technology and AI

Background

In October 2024, LeO updated the OLC board on ongoing digital technology implementation within LeO and its initial approach to AI, specifically seeking the board's view on its appetite for the strategic use of AI. The board agreed that LeO should adopt AI but emphasized the need for a well-considered approach that leverages technology to achieve the 2024-27 OLC strategic aims. LeO’s Executive committed to providing a more detailed update on the strategic approach.

Since October, LeO has developed a draft strategy aimed at building a robust foundation for developing digital solutions, including AI. Alongside this, LeO has established a governance framework to ensure that our approach addresses the moral, ethical, and legal challenges associated with digital technologies, particularly AI.

Work to this point has been completed with a limited budget, drawing on collaborations and internal skills and expertise. LeO’s recently approved budget takes an “invest to save” approach to AI. With both allocated resource and funding, LeO will be in a better position to accelerate plans for digital transformation throughout 2025/26. LeO is mindful of the clammer to use AI wherever possible. As part of the strategy LeO will assess any technological solutions to ensure that only those projects that offer the most impact will be prioritised.

This paper provides an update on the draft AI strategy and governance framework, outlines the progress made since October 2024, and details our approach for 2025/26 and beyond. Given that AI is an ever-evolving field, LeO must adopt a thoughtful approach to ensure that we maximize our resources while staying at the forefront of technological advancements.

Draft 2025-27 Digital Transformation Strategy

The OLC 2025-27 Digital Transformation Strategy (Appendix 1) is designed to leverage technology to support the Legal Ombudsman’s strategic objectives from 2024 to 2027. This strategy aims to enhance LeO's ability to resolve complaints efficiently and share valuable insights to improve legal services. A key focus is on taking people on this journey by augmenting staff with the right tools and fostering a mindset that embraces innovation. Putting LeO’s people at the heart of this strategy will enhance both customer and employee experience.

A crucial component of this strategy is its strategic approach to Learning and Insight. Though at an early stage of thought, the strategy aims to develop LeO’s capability for the use of AI, with an aim to generate actionable insights that drive sector improvements from the wealth of insight data that LeO has access to. This approach emphasises the importance of using data analytics to identify trends and patterns, providing timely feedback that can be shared with the legal sector. These insights help promote better complaint handling, prevent future complaints, and drive higher standards in legal services, aligning with LeO's commitment to transparency and its role in fostering better legal services for consumers.

This digital transformation strategy aligns closely with the broader OLC 2024-2027 strategy, which emphasises continuous improvement and operational excellence. By integrating AI and automation, LeO aims to streamline processes, reduce manual effort, and enhance the accuracy and efficiency of its services. Specific operational process improvements include automating routine tasks, enhancing data management, and supporting decision-making processes. These initiatives not only improve efficiency but also empower staff by providing them with advanced tools, enabling them to focus on more value-added tasks to deliver a more productive efficient service.

LeO recognises that knowledge, skills and expertise in this fast-evolving field are essential to deliver ambitious aims. Therefore, collaboration across the Ombudsman and complaints sector is essential to seek wider solutions and best practices. By collaborating with other organisations, LeO can leverage shared expertise and innovative approaches to enhance its digital transformation efforts. This collaborative approach ensures that LeO can implement effective and sustainable solutions, drawing on the collective wisdom and experience of the sector. Additionally, creating the right balance between in house research and delivery versus procurement from external specialists will be critical in ensuring that LeO offers value for money in its Invest to save budget.

Key Initiatives and Progress

Legal Checks: To effectively leverage AI, LeO needed to be aware of the potential challenges associated with using its data to train AI models and ensure the integrity of its data. Since October, LeO has sought KC advice regarding its ability to operate AI in compliance with the Legal Services Act. This advice has confirmed that LeO is operating within the legal framework and that any potential AI outputs can withstand legal scrutiny. Additionally, LeO is committed to using data ethically and morally, ensuring that all AI applications respect privacy, fairness, and transparency.

Consultancy Engagement: We engaged Audacia, a specialist IT consultancy to identify areas for implementing digital solutions and began exploring proofs of concept. This aligns with a lean process review that pinpointed bottlenecks in the investigation process where technology could expedite cases and free up resources for critical analysis of evidence. Initiatives include using generative AI for written work and technology for evidence bundling and review. These efforts are expected to result in faster case resolution, improved resource allocation, and enhanced focus on critical tasks.

Governance Framework: LeO has established a robust governance framework (Appendix 2) for AI by seeking best practices from external specialists and GOV.UK guidance. This approach ensures that AI development and implementation is ethical, transparent, and secure. By consulting experts and aligning with the UK's pro-innovation regulatory principles. LeO will embed responsible AI practices across the organisation. This comprehensive governance framework supports LeO's commitment to privacy, fairness, and accountability in all AI applications.

Embedding AI Culture: We have started embedding an AI culture by training Executive and operational leads through an intensive five-day strategic AI course. This provided a solid foundation for understanding AI's potential. Additionally, all Corporate Managers and Team Leaders received AI training to develop awareness and identify issues that technology can address, as well as dispelling myths around AI. This initiative aims to increase AI literacy, better identify AI opportunities, and foster a more innovative organisational culture.

GIAA Generative AI Tool: We progressed the development of a generative AI tool to support the initial drafting of reports on service complaints, which then frees up writing time for service complaints team members to ensure accuracy. Proof of concept work has been completed and the tool is now being developed for live implementation, promising enhanced efficiency in report generation and improved accuracy This is expected to go live towards the end of Quarter 1

Website Integration: A direct link from LeO's online complaint form to the case management system has been built and is currently in testing. This seamless integration is expected to go live in May, offering quicker data analysis, reduced manual workload, and improved data quality. Additionally, it is expected to increase the rates of EDI data capture by automating relevant questions in the complaint form, removing an historically paper-based process with low customer response rates.

Final Decision Summarisation Tool: The development of a generative AI tool for summarising Ombudsman final decisions has successfully reached the proof-of-concept stage. However, due to recent changes in LeO's budget and transparency agenda, this project has been temporarily paused. A further review is planned to explore additional functionalities, including the summarisation of case studies and public interest decisions.

2025/26 Next Steps

As part of the Lean Process and Audacia reviews, LeO identified four areas of focus for automation and AI usage in 2025/26 that would have the most benefit for operational efficiency, whilst delivering enhancements to staff experience.

Writing Engine: LeO has begun developing a writing engine for the service complaints team in collaboration with GIAA. Now, LeO plans to create an in-house engine for Operations. Since written work takes up a significant portion of an Investigator's time, this engine will need to be adaptable to all written templates and user-drafted documents, starting with investigator case decisions. The goal is to ensure consistency in written style and readability across investigations, making complex documents easier for readers to understand. This consistency should also produce structured, searchable data, aiding Learning and Insights analysis.

Evidence Bundling and Identification: Investigator feedback and previous case data analysis have shown that evidence requests, collation, and bundling are resource-intensive and administrative tasks with over 40% of live in-depth investigations bottlenecked at this stage at any time. Investigators often sift through unnecessary information, causing delays in the In-Depth investigations process. LeO is working with Audacia to develop proof-of-concept ideas to streamline this process, aiming to reduce investigator workloads and speed up investigations.

General Enquiries Email Management: Currently, LeO uses Outlook to manage emails, with a GET Advisor manually creating new cases and sorting emails into various workstreams. The proposed solution involves automating email integration into the Case Management System, automatically creating cases, and researching ways to reduce or eliminate manual email sorting. This aims to save resources for both consumers and GET Advisors and minimize user input errors that lead to re-work.

AI Embedded Knowledge Search: LeO has a vast library of technical and process guidance for Investigators, but its basic search function makes accessing guidance challenging unless users know specific details. This leads to investigators seeking advice from Ombudsmen, taking up valuable time. Embedding AI into the search functionality aims to provide more accurate results, allowing users to ask less structured questions to find the information they need. Not only would this empower our investigators, it also has the potential to free up Ombudsmen for more value-added work.

Additional Developments

In addition to these operational efficiencies, LeO has identified additional areas that with further development it believes efficiencies could be supported across all areas of the business.

Co-Pilot Licenses: LeO has trained many Executive, Operational, and Corporate leaders on the benefits of AI and automation. To maintain the momentum of digital culture, LeO has acquired co-pilot licenses. The selected AI engine suits LeO's Microsoft environment, balancing user functionality with data security. Using copilot ensures that data remains within LeO and is not used in broader language model development. It is expected that with access to Co-pilot and working within LeO’s AI governance policy, these staff will have more freedom to experiment with AI, discovering ways that individual workloads can be supported. Feedback loops for those involved, means that any solutions that can be replicated trailed across wider groups before being rolled out. This is intended to create a self-directed ecosystem of AI adoption across the business.

Structured Data: LeO has improved its data reporting capabilities, using structured performance data to identify key themes in Operational and Learning and Insight areas. However, extracting further insights requires significant manual data analysis. Important complaint details are often in PDF and Word documents, making analysis difficult. LeO aims to structure this valuable data directly in its Case Management System, facilitating analysis and AI-generated written work. This aims to save time and resources, allowing staff to focus on actionable improvements.

GovAssure: GovAssure is a government assurance process designed to prioritise cybersecurity, protect sensitive data and access and implement best practice. LeO has engaged Actica, an external specialist, to assess the impact of GovAssure. The assessment shows that LeO is well-prepared to complete the review stages, offering valuable challenges and learning opportunities. Although not directly part of LeO’s transformation strategy, GovAssure is a mandatory process that requires significant resources. Further details, including OLC board responsibilities, will be provided in the coming months.

Business Intelligence Development: LeO plans to procure analytics software to deliver timely operational data and insights into complaints. This involves developing existing BI and IT staff to fully utilise available software, aiming to eliminate manual data analysis wherever possible. This supports the people sections of both LeO's People and Technology strategies.

OFFICE FOR LEGAL COMPLAINTS

2025-27 DIGITAL TRANSFORMATION STRATEGY for the Legal Ombudsman

About the Legal Ombudsman

The Legal Services Act 2007 (the Act) established the Legal Ombudsman scheme (LeO) and the Office for Legal Complaints (OLC) to administer it. The Act also established the Legal Services Board (LSB) to oversee the regulation of the legal profession in England and Wales. Both the OLC and the LSB are Arm's Length Bodies of the Ministry of Justice (MoJ). LeO's work supports and aligns with the regulatory objectives.

LeO has two core roles. It resolves complaints about providers of legal services that have not been resolved to customers' satisfaction – as quickly and informally as possible. LeO covers the majority of legal services provided in England and Wales. The rules and limits about what complaints LeO can help with are set out on LeO's website.

The second vital part of LeO's work is sharing learning and insight from the complaints it sees. This promotes better complaint handling, prevents future complaints and helps drive higher standards in legal services.

About LeO's 2025-27 Digital Transformation Strategy

The Legal Ombudsman's (LeO) 2025-27 Digital Transformation Strategy is designed to leverage technology in support of LeO's 2024- 2027 strategic objectives. This strategy, running from 1st April 2025 to 31st March 2027, aligns closely with the Office for Legal Complaints' (OLC) 2024-2027

strategy and aims to enhance LeO's ability to resolve complaints efficiently and share valuable insights to improve legal services.

The digital transformation strategy focuses on six key aims:

- Enhancing customer and employee experience
- Aligning technology with processes
- Improving data analytics capabilities
- Fostering innovation and collaboration
- Proactively seeking knowledge on technological advancements
- Adopting integrated digital solutions

By implementing these aims, LeO aims to become a leading and trusted Ombudsman scheme, where every complaint contributes to driving better legal services. The strategy emphasises a 'digital first' mindset, supporting the customer journey through technological enablers and improved data analytics to provide actionable insights both internally and externally.

Legal Ombudsman longer term strategic approach

LeO's 2025-27 Digital Transformation Strategy looks to leverage current technologies within a rapidly evolving technologic landscape, complimenting LeO's 2024-27 strategy. Throughout the planned strategy period LeO will be assessing what the longer-term future for LeO looks like in a landscape that could potentially see seismic shifts in the way LeO delivers its service.

With the shift to AI and automation, like most organisations LeO must use this period to carefully assess how it implements more perceived radical solutions. This current strategy seeks to improve LeO by become more efficient using AI augmentation and automating tasks. Shifting beyond this approach in the longer term will require LeO to develop an approach that delivers solutions that are ethical, moral and sit within its current legal frameworks, whilst having the impacts on its people, consumers and legal service providers at the heart of any future decision making

OLC Digital Transformation Strategy for 2025-27: overview

Purpose and what LeO is here to do					
Resolving consumer complaints about legal providers, and sharing insight to improve legal services					
Vision and where LeO is heading					
A leading and trusted Ombudsman scheme where every complaint helps drive better legal services					
Strategic objective for LeO's Digital Transformation					
Leverage technology to support the efficient delivery of LeO's strategic objectives					
Aims					
Enhance the customer and employee experience	Align the right technology to the right process across all business areas.	Improve Data Analytics capability to provide actionable insights	Foster a culture of innovation and collaboration	Proactively seeking knowledge on technological change	Adopt Integrated Digital Solutions to Foster a Digital-First Mindset
Enablers					
People culture and change management					
Resources and governance					
Systems and intelligence					
Relationships and collaboration					
Supporting strategies					
People					
Equality, diversity and inclusion					
Future ways of working					
Learning and Insight					

Context for the OLC's 2025-27 Digital Transformation strategy

In the rapidly evolving digital landscape, LeO recognises the need for technological advancement to meet the changing expectations of consumers and legal service providers. This strategy is developed in response to several of the key factors:

- The increasing demand for efficient and accessible complaint resolution services
- The growing importance of data-driven insights in improving legal services
- The potential of artificial intelligence and automation in enhancing organisational efficiency
- The need for robust cybersecurity measures to protect sensitive information
- The shift towards remote and flexible working arrangements

Demand for LeO's service is increasing as more consumers complain about the service they have received from Legal Service providers

- Demand has increased by 30% since 2019/20
- In 2024/25 demand for in depth investigation increased by 20% on the previous year
- Expected demand reductions from interventions such as changes to Scheme Rules time limits have been absorbed by increases in sector led demand
- LeO has adapted to manage increased demand, but a significant transformation is necessary to meet future growth expectations while reducing the number of consumers waiting for its services.

These statistics underscore the need for LeO to embrace digital solutions to enhance its service delivery and impact in the legal services sector.

Strategic objectives

Strategic objective for LeO's Digital Transformation

Leverage Technology to support the efficient delivery of LeO's strategic objectives

The outcomes we are aiming for over the strategy period.

- Embed Intelligent Automation (IA) and Artificial Intelligence (AI) to deliver consistent, repeatable and transparent outputs.
- Using technology to create future capacity to absorb volatility and increased demand while maintaining reductions in unallocated investigations.
- Protects limited LeO resource by aligning impactful solutions to specific high impact problems identified by improved data analytics
- Use technology to deliver analytics that serve to drive timely and impactful Learning and Insight data that drive sector improvements.
- Increase the use of technology solutions to increase efficiency and reduce the process overhead of tasks that can be better achieved through Intelligent Automation (IA) and Artificial Intelligence (AI), across all business areas, allowing users to focus on value-add tasks.

Strategic Aims

Strategic aims under this objective

Enhance the customer and employee experience.

By supporting the customer journey through technology enablers, this strategic aim is about how LeO delivers its service. With a focus on improving the user experience, implementing strategies and technologies that improve interactions and, satisfaction for both customers and employees.

For customers, this means providing a seamless, efficient, and fair service that responds to their needs and expectations. For employees, it involves creating a supportive and engaging work environment that fosters productivity, well-being, and professional growth.

Align the right technology to the right process.

We will select and implement technology solutions that best fit the specific needs and requirements of each business process, ensuring that technology enhances efficiency, accuracy, and effectiveness, rather than complicating or hindering operations, by carefully matching technology to the process as well as matching processes to technology.

Improve Data Analytics capability to provide actionable insights.

Enhancing the tools, techniques, and processes used to collect, analyse, and interpret data. This improvement ensures that data analytics not only identifies trends and patterns but also delivers clear, actionable recommendations that can be implemented to achieve better outcomes. These insights will serve two primary purposes:

- Internal Learning: Providing valuable feedback to improve LeO's operational efficiency, decision-making processes, and service quality.
- External Learning and Insight: Sharing aggregated, anonymised data and insights with the legal sector to drive improvements in legal services and complaint handling practices. This aligns with LeO's commitment to transparency and its role in fostering better legal services for consumers.

Foster a culture of innovation and collaboration.

By creating an environment where creativity and teamwork are encouraged and supported and implementing practices and technologies that facilitate open communication, idea sharing, and joint problem-solving. By promoting a culture where employees feel empowered to experiment and collaborate, LeO aims to drive continuous improvement, generate innovative solutions, and achieve greater success.

Proactively seeking knowledge on technological change

This aim involves continuously staying informed about the latest advancements and trends in technology. This means actively investing in and modernising LeO’s digital infrastructure to ensure robust, secure, and scalable technology solutions that support LeO’s strategic goals, through research, attending industry events, participating in training, and engaging with experts to understand how innovative technologies can be leveraged. By doing so, LeO can anticipate changes, assess and adapt quickly to absorb volatility and increased demand while maintaining reductions in unallocated investigations.

Adopt Integrated Digital Solutions to Foster a Digital-First Mindset

We will implement cohesive and comprehensive digital tools and platforms across LeO, ensuring that all systems are interconnected and work seamlessly together, promoting efficiency and ease of use. By prioritising digital solutions and encouraging their use, LeO can create a culture that embraces technology, drives innovation, and enhances overall performance.

Strategic enablers

Enablers are the capabilities we need to fulfil our purpose, achieve our objectives and move toward our vision.

People Culture and Change Management

A culture that is open to change is crucial for the success of digital transformation, empowering employees with the necessary skills and fostering a collaborative culture is vital. Encouraging agility, adaptability, and recognising innovation are important change management strategies that will help overcome resistance ensuring a smooth adoption of innovative technologies.

- Foster a culture of collaboration, innovation and continuous learning.
- Upskill and reskill employees to equip them with new digital competencies.
- Implement clear communication strategies to explain the benefits of digital change.
- Recognise and reward innovation and digital initiatives while addressing resistance proactively through targeted change management tactics.

Resources and Governance

The proper allocation of resources and clear governance structures ensure that digital transformation initiatives are aligned with LeO's Strategic goals. Effective resource management, from budgets to talent alongside strong transparent governance, guide and support LeO's decision-making and accountability.

- Allocate dedicated budgets and resources to digital projects.
- Establish internal governance frameworks to ensure strategic alignment and accountability as well as regulatory compliance.
- Collaborate with allied organisations to share expertise and resource to solve common shared problems
- Monitor and evaluate resources to ensure optimal use.

Systems and Intelligence

The backbone of digital transformation is the integration of advanced systems and intelligent technologies. Leveraging data, AI, and Intelligent Automation solutions enables smarter decision-making, enhanced operational efficiency, and a better customer experience.

- Implement robust cybersecurity measures to protect digital assets.
- Integrate and adopt emerging technologies such as AI and machine learning to improve process automation and productivity.
- Harness data analytics to generate actionable insights and drive decisions.
- Deliver a seamless and efficient customer engagement through automated tools and services that integrate with existing processes and applications

Relationships and collaboration

Developing internal and external partnerships and teamwork, drives innovation and organisational excellence. Fostering trust, transparency, and shared goals across departments and external partners ensures alignment and accelerates transformation.

- Build a collaborative ecosystem by nurturing relationships with internal teams, technology partners, allied organisations and stakeholders to align objectives and leverage collective expertise.
- Encourage knowledge-sharing through cross-functional workshops, digital platforms, and open communication channels to break down silos and spark innovation.
- Establish clear communication norms: define roles, decision-making processes, and feedback mechanisms to ensure cohesion and accountability.
- Leverage digital tools like collaborative software (e.g., MS Teams, DevOps), to streamline workflows and maintain real-time visibility across teams.
- Encourage a culture of openness and empathy where teams can share challenges and feedback, identifying interdependencies and recognise and celebrate team achievements to reinforce trust, motivation, and a culture of shared success.

AI Governance Framework

Version Date: March 2025

Version: 1.1

Approved by:

Policy Owner: ICT Manager

Review date: March 2026

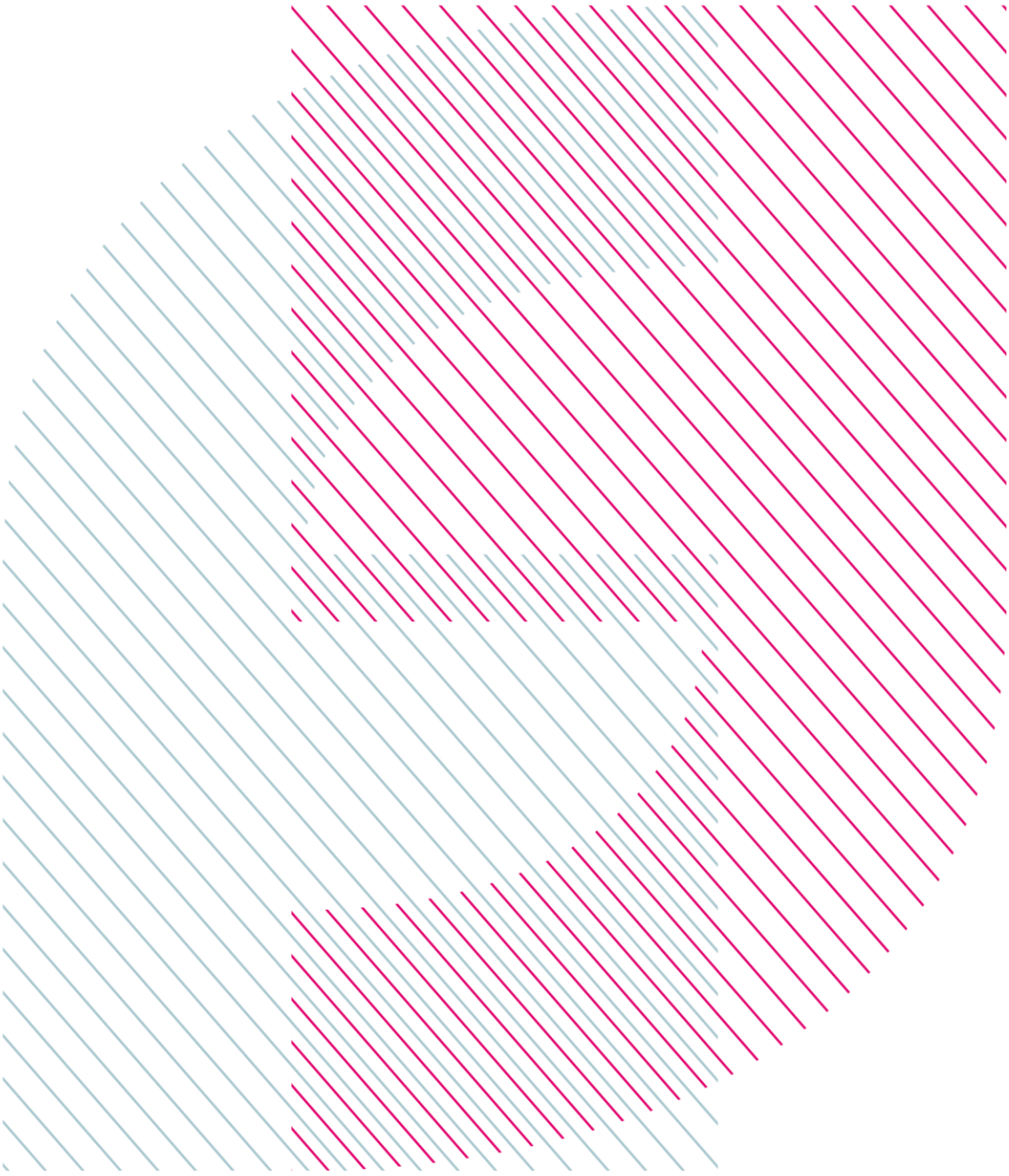

Table of Contents

Latest update

Version	Date (dd/mm/yy)	Summary of Changes	Actioned by (role)
1.0	04/03/2025	Original Policy	
1.1	03/04/2025	LeO revision	ICT Manager

Purpose

Our AI Governance Framework sets out our commitment to ensuring the responsible, ethical, and compliant use of Artificial Intelligence (AI) in our operations. It is designed to align with legal, regulatory, and ethical standards while fostering trust, accountability, and transparency in AI-driven processes.

Its purpose is to ensure that everyone involved in the selection, deployment, and use of AI at LeO is fully aware of their responsibilities.

For this policy, “AI systems” include all technologies and applications that involve automated decision-making, machine learning, natural language processing, and other AI-driven functionalities that influence business operations and customer interactions.

Scope

All those employed, engaged by, or working on behalf of LeO are required to comply with this AI Governance Framework. This includes agents, consultants, contractors, suppliers and those employed under a contract of service. The framework should be read in conjunction with the Information and Data Protection Policy, Security Policy, IT Acceptable Use Policy and Access to Information Policy.

Principles

These AI Principles have been defined to help LeO assess, select and oversee AI technologies that align with both our regulatory obligations and our organisational values to be Open, Independent, Effective and Fair.

Ethics: LeO will only adopt AI technologies that align with our values, prioritising fairness, non-discrimination and responsible use to prevent harm or bias.

Accountable: LeO Is fully accountable for all AI-driven decisions and will ensure that human oversight is in place to validate outcomes and address risks.

Secure, Private & Legally Compliant: AI technologies must meet LeO’s security and privacy standards as defined in the Data and Information Policy and Security Policy, ensuring compliance with the Legal Services Act (LSA) 2007, UK GDPR and any other applicable laws, so that we can protect sensitive data and uphold the trust of our stakeholders.

Transparent: LeO will use AI technologies that provide clear, explainable decision-making processes, allowing users to understand how AI-driven outcomes are reached.

Responsibilities

It is the responsibility of **all members of staff** to:

a) Read and follow the organisation's AI Governance Framework.
b) Only use approved AI technologies for their stated purpose(s) as listed in Section 1.1
c) Review the accuracy of AI generated outputs and decisions prior to storing or sharing the output, both internally and externally.
d) Adhere to LeO's AI Principles, taking the appropriate steps to ensure that our use of AI is ethical, secure and transparent, and that we are accountable for its use within our organisation.
e) Read and follow related policies, such as the Data and Information Policy and Security Policy, and any supporting guidance.

A full breakdown of Roles and Responsibilities to manage and oversee our AI Governance Framework is set out in Appendix 2.

Policy Statement

The Legal Ombudsman (LeO) recognises the potential of Artificial Intelligence (AI) to improve efficiency and support our operations. As the organisation harnesses these opportunities, it is essential that we use AI responsibly, which is paramount to maintaining the confidence of our customers, employees and stakeholders.

This AI Governance Framework exists to ensure that LeO designs, implements and uses AI in accordance with our principles to be ethical, accountable, secure and transparent.

LeO is committed to ensuring that all staff understand the risks and limitations of using AI. Training, guidance and oversight mechanisms will be in place to support the responsible use of AI.

1. AI Technology Policy

This section outlines the AI technologies that are approved for use within LeO and staff responsibilities when using AI.

Approved Technologies

The following AI technologies have been approved for use within LeO for the stated purpose(s).

Technology	Use Case
M365 Copilot	Support of office and non-casework tasks
GIAA document draft	GIAA empowered draft service complaint response document
Perplexity.AI	Support research of office and non-casework activities

1.1 Prohibited Technologies

Staff may only use AI technologies listed in section 1.1, and only for approved purposes. Unlisted and unlicensed AI technologies must not be used for work purposes on LeO IT equipment or personal devices. Accessing unlisted AI technologies on any LeO-owned device (e.g., laptops, phones, tablets) is not permitted.

The following AI technologies have been prohibited for use within LeO for any purpose

Technology	Engine
AI Chat tool	DeepSeek AI or any model that uses the DeepSeek engine

1.2 Staff Responsibility for AI Use

Staff are fully responsible for the generative outputs and decisions produced while using AI. This includes:

- Verifying accuracy – ensuring AI generated content is factually correct.
- Compliance – outputs must adhere to organisational policies and regulatory obligations.
- Ownership – staff are responsible for monitoring the language, tone and grammatical accuracy of outputs, such that they are of a standard they would be happy to share had they written it themselves.

Staff understand that LeO do not use AI technology to replace human-decision making. UK GDPR (Article 22) states that individuals have the right not to be subject to solely automated decisions with legal or significant effects.

Staff will refer questions regarding AI technologies and their appropriate use to their line manager.

1.3 Transparent AI Use

LeO will communicate with customers, professionals and other stakeholders about where and how we use AI technology. This is important to maintain trust and confidence in our services, by being clear when AI has supported our work and reassuring people that final decisions are always made by people.

2. Security Incident Management

2.1 AI Technology Risks

The use of AI introduces new data protection risks, and staff must stay vigilant to uphold the integrity of our customer's data.

Some risks relate to the outputs and decisions generated by the AI Technology, these can include:

Biased or unfair outputs: This is when AI outputs are explicitly influenced by known characteristics of a data subject, leading to unfair or discriminatory outcomes. For example, an AI model assumes higher reliability in evidence submitted by professionals, compared to that submitted by the public.

Data Inference: Unlike direct bias, this occurs when AI infers characteristics based on patterns in the data it processes. This can lead to unintended assumptions and discrimination. For example, an AI system has inferred a person's race based on correlations between their address and the nature of their complaint, even though race is not explicitly provided as an input.

If staff identify bias, inaccuracies, or inappropriate content in generative AI outputs, or suspect an issue with the technology, they are required to report it to IT Support by email at the following address: it.servicedesk@legalombudsman.org.uk or, alternatively, using the support portal found at the URL, https://thelegalombudsman.happyfox.net/https://thelegalombudsman.happyfox.net/

Further risks using AI can result from human error, such as:

Unintended Disclosure: This occurs when sensitive, personal or confidential information is accidentally exposed through AI. For example, a staff member has input personal data about a customer into a non-secure large language model (LLM), e.g. a free-to-use personal account in ChatGPT.

Automated Processing: Occurs when a biased, unfair or inferred decision or output is not rectified due to insufficient human oversight. For example, a staff member has failed to review the accuracy, compliance or appropriateness of an AI generated output or decision.

2.2 Personal Data Breaches

The risks outlined above can lead to a personal data breach without proper oversight. LeO defines a personal data breach as a security incident that affects the confidentiality, integrity or availability of personal data. LeO's policy for reporting security incidents is outlined in the Information and Data Protection Policy.

3. Assessment and Approval of new AI Technology

LeO is accountable for the AI that we use, and when there is an opportunity to improve our service using AI, the technologies that are considered are assessed as part of a consistent, repeatable process.

3.1 Simple AI Solution Examples

Correspondence Sentiment Analysis

LeO wishes to use an LLM to assess the overall sentiment of correspondence submitted as case evidence. As a first step, the desire is to input a piece of correspondence to a model and have it return sentiment scores.

When selecting an AI solution to assess the sentiment of correspondence, LeO must ensure the model is ethical, fair, and regularly audited to mitigate bias, particularly given the sensitive nature of legal complaints. The system must be accountable, allowing human review and correction of outputs, with robust monitoring and logging to address errors and unintended consequences. It must comply with all security and privacy obligations, including being hosted within LeO's Azure environment and processing only necessary data. Finally, the AI must be transparent, using explainable and verifiable training data, with clear information on how data is handled and stored.

LeO decides to use the "Sentiment analysis and opinion mining" tool as part of the AI language services provided by Azure. As Microsoft provides clear documentation on how these models are trained and maintained, LeO is assured that this choice meets its standards for ethical use, accountability, security & privacy, and transparency.

Complaint Topic Classification

LeO wishes to use an LLM to automatically classify incoming complaints into specific categories, such as "Delay," "Costs," "Communication," or "Conduct." As a first step, they want to pass the complaint text to a model and have it return a clear topic label to help route cases to the appropriate team more efficiently.

When selecting an AI solution for this purpose, LeO must ensure it is aligned with its core AI principles. The technology must promote fairness and prevent discrimination by avoiding biased classification results; it must maintain human oversight, so that AI-generated classifications can be reviewed and corrected where necessary; and it must comply with strict privacy, security, and legal standards, including UK GDPR and the Legal Services Act 2007, to ensure the protection of sensitive personal data. Additionally, the model must offer transparency in how it was developed and how it reaches its conclusions, supporting trust and explainability in decision-making.

LeO decides to use Azure AI Language's "Custom Text Classification" service to train a model on their own complaint data. Because this service is securely hosted within Azure and gives LeO full control over their training datasets, it meets LeO's commitments to ethical, accountable, secure, private, and transparent AI use.

3.2 Assessing Technologies using AI Principles

LeO's AI principles exist to help assess the suitability of new and existing AI Technologies.

3.2.1 Ethical

Ethical and responsible use of AI is critical for LeO to maintain the trust of customers, the legal sector and the public. AI technologies used by LeO must be committed to displaying and upholding high ethical standards.

AI technologies will be assessed on evidence that the model is ethical and fair, good examples of this can include:

- Evidence that bias is actively mitigated, by using diverse training datasets, implementing features that avoid reinforcing biases and conducting regular bias audits.
- Decisions made by the model align with ethical and legal standards.

3.2.2 Accountable

AI technologies will be able to evidence that they are accountable for the outputs and decisions of the model. This includes taking pro-active steps to address issues and refine outputs.

Examples of Accountable AI practices include:

- Features exist to refine outputs, so that inaccuracies can be corrected
- Monitoring and logging features exist so that unintended consequences can be identified, and corrective action can be taken.

3.2.3 Secure & Private

To mitigate risks associated with unvetted AI tools, all staff must use only LeO-approved AI systems where data is constrained within LeO's **Microsoft 365 boundary**. This restriction ensures compliance with internal security, data protection, and ethical standards, as well as legal obligations under the **Legal Services Act 2007**, **Data Protection Act 2018**, and **UK GDPR**.

Key Requirements for Approved AI Technologies:

- **Data Ownership**: Models must ensure LeO retains full ownership of all data processed, preventing unauthorised use of confidential information for unsuitable purposes.
- **Data Minimization**: AI tools must be designed to process only necessary data, with personal data anonymised or encrypted where possible.
- **Regulatory Alignment**: Systems must adhere to the UK's AI regulatory principles (safety, transparency, fairness, accountability, and contestability).

Exceptions Process:

- Departures from approved systems require written authorisation from the ICT manager who will inform the executive of any departure.

- Approved exceptions must undergo a documented risk assessment, including a **Data Protection Impact Assessment (DPIA)** and validation of compliance with the above requirements.
- Unauthorised use of external AI tools (for example, public LLM's, AI Chat models) is prohibited due to risks of non-compliance (for example with, GDPR) and intellectual property exposure.

3.2.4 Transparent

AI technologies used by LeO will be transparent in how they handle data and select training sources for their model. The outputs of the model will be explainable and reproducible.

Examples of transparency in AI technologies include:

- Models are trained using verifiable and appropriately sourced data, so that the model is not reliant on hidden, or undisclosed data sources.
- Data usage policies are openly communicated so that users understand the types of data being collected, how it is stored and how long it will be stored for.

3.3 Key Implementation Questionnaire

The following questionnaire should be completed when assessing the **suitability of adopting an AI system into your current process** within LeO. These questions have been chosen to reflect our guiding principles. You MUST be able to confidently answer "Yes" to all questions for the AI system to be considered for implementation.

Questions	Answers		Comments & Justifications
	Yes	No	
Have you evaluated the AI system's capabilities against your implementation goals, and does it add measurable benefits?			
Can you be sure that the AI system will not use your data for further model training?			
Can you be sure that the AI system has been trained in a way that mitigates bias?			
Is there a process in place that allows the user to override the AI systems output?			
Are you able to access (or account for) the source data used to train the AI system?			
Will the decisions made by the AI system align with LeO's ethical and legal standards?			
Is the AI system output visible to the user, with reviews in place to monitor its accuracy?			
Is the AI system's data processing pipeline in full alignment with LeO's data usage policies?			

Is the AI system trained effectively for the tasks in the current workflow? i.e. it is trained to classify and will be classifying documents.			
Are there strict access controls for the AI system that ensures only authorised personnel/systems can view/manipulate sensitive data?			
Is this the most well-established AI system for the current workflow and task?			

Table 1 - Key implementation questionnaire.

3.4 Risk Of Implementation Questionnaire

The following questionnaire should be completed when evaluating the **risks that could be introduced when adopting the AI system into your current process and** assumes that it has passed the Key Implementation Questionnaire**.** These risks have been chosen to reflect our guiding principles. Give informed and accurate scores to the considerations and use the total to evaluate the overall risk of the AI system to LeO and the integrated process(es).

Total Score	Maximum Individual Risk Score	Implementation Action
0-13	1	Progress to implementation – May be ran as project or through BAU, AI system poses little to no risk to LeO
14-26	3	Review with Exec Team – Must be ran as a project, AI system poses some risk to LeO
27+	4	Do not implement – AI system poses considerable risk to LeO

Table 2 - Implementation actions based on risk of implementation questionnaire scores.

Risk Considerations	Risk Score				
	No Risk	Low Risk	Medium Risk	High Risk	Very High Risk
	0	1	2	3	4
The data being passed to the AI system is highly unstructured and of poor quality.					
The AI system is static and won't scale with the growth of the business.					
The AI system will have to process highly sensitive, personal and private data.					
The AI system has no documentation or training regarding its use and implementation.					
You find no evidence of reputable industry analyses, awards, or user reviews that endorse the AI system.					

A lot of additional work will be required to implement the AI system seamlessly with current workflows.					
Implementing the AI system will require additional internal training or change management.					
As legal requirements evolve, the AI system won't obviously adapt to any new changes.					
There is direct contact between the AI system and our customers that could affect relations.					
The impact of adopting the AI system is widespread and affects more than the intended workflow.					
The AI system usage is buried within other systems, with no user-friendly front-end integration.					
Decisions made by the AI systems are difficult to trace back to specific data points or are obscured by the model itself.					
When improving the current workflow/task, the AI system could introduce inefficiencies in other areas.					
TOTAL SCORE:					

Table 3 - Risk of implementation questionnaire.

4. Monitoring and Oversight

All users of the AI technology within LeO are responsible for monitoring its output in deployment. Any concerns should be reported immediately to the IT Service Desk. The following section indicates how LeO can ensure reliable and accurate performance from any deployed AI system, with proactive and evaluative measures.

4.1 Continuous Performance Monitoring

Regular system audits should be completed to evaluate the ongoing accuracy, fairness and effectiveness of AI outputs.

During deployment of the AI system, define a set of key performance indicators and acceptable performance thresholds. These can be used to benchmark the model performance at agreed intervals.

Where possible, deploy automated logging of system behaviours, especially for critical decisions where traceability is key.

4.2 Risk and Impact Assessment

The IT Operational Manager should conduct periodic risk assessments of current AI-use cases. These should account for any potential harms or biases introduced by the AI system whilst evaluating any unintended consequences of its deployment.

New scenarios are periodically tested against the current AI systems to make sure they don't produce erroneous results, and that the systems maintain a reasonable level of robustness.

4.3 Human Oversight and Intervention

All members of LeO that use deployed AI systems are made aware of their accountability when supervising AI decisions. The IT Operational Manager should make all members aware of the clear escalation procedure if they suspect any anomalies within the AI systems.

Review mechanisms are in place for high-risk AI outputs. As a minimum, this should involve a human-in-the-loop review process for critical decisions, or any time an AI system is acting on behalf of the user.

All users should be made aware of human override or deactivation procedures where necessary.

5. Education and Training

The IT Operational Manager shall, in conjunction with Human Resources, implement a training programme for staff, and if required, provide information and further training in AI Technology and its secure use to meet specific requirements.

Related documents

LeO's Information and data protection policy sets out how we ensure information is handled, stored, processed, and transmitted securely. All staff are required to always consider the most appropriate security measures.

This policy should be read in conjunction with the Information and Data Protection Policy.

Further information

If you have any queries, PLEASE contact the Head of IT, SIRO or the Information Rights and Security Team - infosec@legalombudsman.org.uk.

Appendix 1

AI Term Glossary

Term	Definition
Artificial Intelligence (AI)	A system or technology that simulates human intelligence to perform tasks such as natural language processing, data analysis, and decision-making.
Machine Learning (ML)	A subset of AI that enables systems to learn patterns from data and improve over time without being explicitly programmed for each scenario.
Large Language Model (LLM)	A type of AI model trained on vast amounts of text data to understand, generate, and analyse human language with a high level of accuracy.
Generative AI	AI systems capable of generating new content, such as text, images, or audio, based on learned patterns from training data.
Natural Language Processing (NLP)	A field of AI focused on enabling machines to understand, interpret, and generate human language.
Automated Decision Making (ADM)	The use of AI or algorithms to make decisions with little to no human intervention.
Human-in-the-Loop (HITL)	AI systems that incorporate human oversight in decision-making processes.
Data Privacy	Protection of individuals' personal and sensitive data processed by AI systems.
Model Drift	The gradual degradation of an AI model's performance over time due to changes in the underlying data distribution
Risk-Based AI Governance	A framework that assesses the risks associated with AI applications and establishes appropriate safeguards.
Transparency	The principle that AI decision-making processes should be understandable and accessible to stakeholders.
Explainability	The ability to understand and interpret how an AI system reaches its conclusions.
Data Poisoning	AI has learnt incorrect or biased patterns due to malicious actors intentionally inserting false, misleading or corrupted data into the training dataset.

Appendix 2

Roles and responsibilities for AI Governance

The roles and responsibilities defined for data and information protection are extended to include AI Governance, which is part of data/information assurance.

Role	Responsibilities
Chief Ombudsman	Corporate Oversight and Accounting Officer implications
Executive Team	Provides strategic leadership for AI governance, ensuring policy compliance, business priorities, and regulatory obligations while overseeing risk mitigation and stakeholder engagement
Senior Information Risk Officer (SIRO)	Is responsible for the overall governance and management of risks associated with AI systems.
ICT Manager	Supports the Executive with the development of AI systems, ownership, procurement.
Budget Holder	Supports the responsible fiscal management of the AI product(s)
Risk Owner	Supports the consistent and robust identification and management of opportunities and risks within desired levels (risk appetite) in pursuit of our AI objectives
Information Asset Owner (IAO)	Responsible for ensuring that data assets are protected by appropriate physical and technical controls to prevent accidental/deliberate loss or damage to data.
Data Protection and Information Compliance Officer	The Data Protection and Information Compliance Officer will ensure LeO is supported to achieve organisation compliance with the laws and regulations relating to data protection liaising with key staff i.e. SIRO, Chief Ombudsman, Deputy Chief Ombudsman, and other members of the Executive team.
Staff and all Third Parties	All staff within the organisation have a responsibility to ensure they comply with this policy and any associated policy, guidance or process. Staff will provide feedback and insights on the effectiveness, usability and impact of AI technologies. Where appropriate, staff will draw responsibilities to the attention of contractors, sub-contractors and applicable third parties. Staff undertaking procurement activities for AI technologies are required to ensure that external AI products and service providers deliver solutions that are aligned with LeO's AI principles.