Parliamentary and Health Service Ombudsman

Artificial Intelligence (AI) ethics and transparency policy

Version 1 | February 2026

1. Purpose

1.1 The Parliamentary and Health Service Ombudsman (PHSO) investigates complaints fairly and impartially. As we embrace digital transformation, Artificial Intelligence (AI) technologies have the potential to improve our efficiency and transparency, and provide better experiences for complainants.

1.2 AI is defined broadly as technologies that mimic human intelligence to solve complex tasks. For example, planning, classification, prediction and content generation.

1.3 While AI presents an opportunity there are also risks and anxieties about its use. It is therefore important that AI is used responsibly, ethically and transparently to maintain trust in our service.

1.4 This policy establishes the framework for the use of AI in our work. It aligns with the AI Playbook for the UK Government. This framework will make sure any AI tools we develop and use are ethical, transparent, accountable and aligned with our values. It supports responsible innovation while looking to safeguard the trust of those interacting with us.

1.5 AI is fast-developing technology so this policy will need frequent amendments. We will make sure version control is updated and a summary of the main changes is added whenever an update is made.

2. Policy objectives and scope

2.1 The purpose of this policy is to define how we will govern, use and oversee AI technologies to allow us to deliver our complaint services more effectively.

2.2 This policy has four main objectives that will:

- safeguard complainants and staff by making sure any AI we use is legally compliant and supports fairness, accountability and transparency
- provide clear guardrails to prevent misuse or misinterpretation of AI outputs and making sure they are reliable and accurate

- align AI practices with UK Government, NHS and Information Commissioner's Office (ICO) guidance
- establish clear governance structures and risk management approaches.

2.3 This policy applies to any use of AI by PHSO. It applies to AI regardless of whether it is developed internally or purchased commercially. The policy covers:

- staff when carrying out a PHSO-related task, including progressing a single complaint (for example, automation of manual tasks, creating a summary or document analysis)
- management of casework (for example, predicting demand to make sure enough staff are available)
- gathering insight from cases (for example, identifying common themes)
- interacting with service users (for example, automated support processes)
- other non-casework uses of AI, such as those embedded within digital service desk tools.

3. Legal compliance

3.1 The legal basis for any use of AI that makes use of personal data or that produces an output that relates to a person must be defined and documented before use.

3.2 Any use of AI products or services which processes personal data must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

3.3 There are specific clauses in Article 22 of UK GDPR that apply to automated decision-making. These clauses give people the right to challenge any significant decision that is made based solely on automated processing of sensitive personal data.

3.4 **'Solely automated'** means no meaningful human involvement. A human must actively review and be able to change the outcome. A **'significant decision'** is one with legal or similarly significant effects on a person.

3.5 There are certain circumstances where automated decision-making for significant decisions is allowed. These are where it:

- is necessary for a contract
- is authorised by law
- has explicit consent.

3.6 Where the specific circumstances apply, UK GDPR sets out safeguards that must be followed. A data controller must:

- inform the individual of the automated decision
- allow them to make representations
- offer the right to human intervention on request
- give them the opportunity to contest the decision.

3.7 We will always consider the legal implications of any use of AI and conduct a Data Protection Impact Assessment (DPIA) and, where necessary, seek appropriate legal advice.

3.8 We will always make sure the necessary legal safeguards are in place before adopting a use of AI that falls within the GDPR definition of automated decision-making.

4. Principles

4.1 Use of AI at PHSO will be supported by following eight ethical principles.

1. **Human oversight and control**
   We will not use AI to make a decision on a complaint that has passed through our triage stage. These decisions will be made by human caseworkers. Where AI is used to assist a caseworker, by providing summaries, recommendations or evidence retrieval, this will be tested and monitored for data quality by humans.

2. **Fairness, equity and quality**
   We will routinely evaluate all AI systems for potential bias to make sure every complainant is treated fairly. We will also monitor and assess the quality and consistency of AI outputs on

an on-going basis, taking action when necessary to maintain our standards.

3. **Transparency**
   Complainants are data subjects and therefore have the right to:
   - know when AI has been used and the role it played
   - know the extent of human oversight applied
   - request a human to review a decision that has been made by AI alone.

4. **Accountability**
   Our staff remain accountable for their decisions on complaint investigations. Using AI as part of a process or workflow does not transfer accountability away from our staff. If AI is used as part of our triage process to make an automated decision, we will be legally responsible for the decisions made and staff will conduct human reviews as part of the necessary safeguards.

5. **Privacy and security**
   Any use of AI must comply with UK GDPR, the Data Protection Act 2018 and our Information Governance policies. Personal data used to train AI must be risk assessed before use and anonymised. Where personal data needs to be used it must be minimised to make sure that only what is required to meet the purpose is used. An AI Output must not be used in ways that impact complainants during testing without human input and review.

6. **Proportionality**
   AI will be used where it can show it supports us to carry out our functions. For example:
   - to improve efficiency, quality or fairness
   - to allow the identification or monitoring of casework risks
   - to help us satisfy legal obligations.

7. **Explainability**
   AI outputs must be easily understood by staff and the complainant.

8. **Sustainability**

Our environmental values will be considered as part of the decision-making around adopting new AI solutions. A clear statement about the environmental impact of an AI solution should be provided by the supplier and documented. If unavailable, we should make attempts to show sustainability. We can do this by comparing the carbon dioxide emissions of the new automated solution compared to the previous approach.

5. Our AI guardrails

5.1 An AI guardrail refers to a set of rules, mechanisms or safeguards designed to make sure that AI operates safely, ethically and within the intended boundaries. These guardrails can be technical, procedural or policy based.

5.2 We have adopted the following guardrails to help prevent harmful, biased or unintended behaviour from the use of AI.

- AI will not be the decision-maker in complaints that have passed through our triage stage.
- All AI outputs used as part of an investigation must be reviewed and validated by trained staff before being included in any formal casework.
- AI solutions will be restricted to data sources that have been through a formal review and deemed to be suitable for AI processing.
- Where necessary, access to AI tools will be role-based with restrictions applied.
- Content that is entirely generated by AI (without human intervention) must be clearly distinguishable from content written by humans. This does not prevent the use of productivity tools, such as those that help with the drafting of documents.
- Personal data in AI prompts must be restricted from general purpose internet access or uncontrolled knowledge sources, unless controls are in place to anonymise personal data.
- AI systems must be assessed for bias and continually reviewed to support equality, diversity and inclusion.

- All prompts, queries, inputs and outputs must be logged for monitoring and audit purposes and retained in accordance with our retention schedule.
- Staff must not input personal, sensitive or confidential complainant data into AI tools that are not approved for organisational use.
- Any new use of AI will be assessed and approved by the AI Governance Board to make sure a proposed solution is explainable and proportional.
- The supply chain for any use of commercial AI products must meet our ethical standards.
- AI will not be used to replace professional advice or to reduce the training and skills requirements of our staff.

6. Responding to concerns

6.1 We recognise that AI is a new technology and many people have concerns about its use. To maintain confidence and trust in our services we will provide clear, plain English explanations of how we use AI, including in our privacy notices.

6.2 Where someone requests an explanation of how AI has been used, we will provide this to them.

6.3 Where AI is used to analyse complaint data after submission as part of demand management, this process (including how it has been reviewed by a human caseworker) will be explained.

6.4 We will regularly publish transparency reports outlining AI use, benefits and risks, aligning with the UK Government Algorithmic Transparency Recording Standard (ATRS). This will include information about human and environmental impacts.

7. Governance and accountability

7.1 We will set up an AI Governance Group. This will be chaired by the Chief Digital and Transformation Officer, with representation from Legal, Information Access and Assurance, Operations, Digital Data and Technology, People and Talent, Quality and Communications teams. The Group will also seek contributions from external stakeholders. It will prepare reports on AI use, benefits and risks for our Audit and Risk Committee

each quarter.

7.2 We will include a summary of our use of AI, including explanations of risks and mitigations and any incidents raised in our annual report.

7.3 Data Protection Impact Assessments (DPIAs) and Equality Impact Assessments must be completed before development and use of any AI product or service.

7.4 The service catalogue must contain the AI tools approved for use at PHSO and include an explanation of how it works and how it will be maintained, aligning with the ATRS.

7.5 We will continually monitor AI performance, accuracy, consistency and fairness, with results published on an internal dashboard.

7.6 Material changes to how an AI tool is used must be assessed and approved before use.

7.7 There must be clear ownership. The Ombudsman remains accountable for casework outcomes. The AI Governance Board is accountable for responsible AI use. Individual staff are accountable for their use of AI tools.

7.8 We may consult with our complainants, advocacy groups and other interested parties when designing or expanding AI use and collect feedback to shape our future AI governance.

8. Risk Management

8.1 AI carries inherent risks. We will manage these through structured processes.

- **Bias**
  We will regularly test AI for unfair bias, with corrective measures applied immediately.
- **Accuracy and consistency**

AI products will be re-tested periodically to make sure they still achieve the required standards as defined by the product owner. AI-generated outputs will be tested by staff to avoid over-reliance on AI in critical decisions.

- **Security**
  All uses of AI will be hosted in secure environments, with access controls, encryption and audit trails, and in locations compliant with UK data protection law.
- **Reputational risk**
  We will actively communicate our uses of AI and implement the required safeguards.
- **Legal and regulatory compliance**
  We will make sure we comply with data protection law, ICO guidance and government standards through audits and DPIAs. We will report any incidents related to use of AI to our Information Access and Assurance team for investigation. For example, an inaccurate summary created by AI which if not checked by a human caseworker and relied upon would impact a complainant.
  Operational risks
  Contingency plans will be in place if a use of AI fails or generates harmful outputs.

9. Training and awareness

9.1 Staff involved in developing and testing AI must have guidance and training on the use of sensitive data and the outputs AI generates.

9.2 AI can only be used responsibly if staff understand its power and limitations. Staff using AI tools for their work will complete appropriate training. We will embed AI ethics awareness into our wider learning and development framework.

9.3 We will provide clear guidance to staff on safe and appropriate use of approved AI tools for casework before they use them. We will also publish guidance on the use of prompts and communication with complainants.

9.4 AI tools will be used to assist our staff to carry out their jobs. Staff must retain the skills required to carry out their role

without AI and new staff will continue to take part in training to a develop these skills.

10. Review and continuous improvement

10.1 This policy will be reviewed annually by the AI Governance Board and approved by the Audit and Risk Committee. It will form part of our information security framework.

10.2 The changing nature and rapid advancement of AI technology, and potential changes to legislation and government guidance, may result in more frequent changes to this policy.

11. Policy or procedure information

Author: Alex Daybank

Related policies and guidance:	• Information Management Policy • Security and Information Incident Management Policy • Privacy Notice • Service Model Guidance • AI Playbook for the UK Government • Algorithmic Transparency Recording Standard (ATRS)

Version control

Date	Version	Content/changes made	Owner of changes	Agreed by:
18/09/2025	0.1	Initial draft	AD	
10/10/2025	0.2	Updated to reflect responses to comments	AD	
21/10/2025	0.3	Further amendments	AD	
03/12/2025	0.4	Additions following Ombudsman review	AD & KC	
19/12/2025	0.5	Updates following ET review	AD	
28/01/2026	0.6	Revisions to language following consultation with Content team	AD	
04/02/2026	1	Final amendments following ET discussion and approval	AD	Executive Team