CENTRIC

Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

AIPAS

AI Accountability for Policing and Security

Guidance for Implementing AI Accountability in Policing

May 2025

Foreword

The integration of Artificial Intelligence (AI) into policing represents a significant development in the evolution of policing practice. While AI offers the potential to enhance operational effectiveness and to improve service delivery, it simultaneously introduces novel and complex challenges to established accountability frameworks.

This guidance has been developed to assist Chief Officer Teams, Enabling Services and Oversight Bodies in navigating these challenges with clarity and rigour. Structured around eight themes, the guidance provides step-by-step recommendations across the AI lifecycle – from design or procurement to deployment, migration and decommissioning – ensuring that AI accountability is embedded at every stage of technological adoption.

Accountability in policing is not optional; it is foundational. The deployment of AI-enabled systems, particularly in contexts involving surveillance, biometric identification or inferential decision-making, requires heightened diligence and transparency. The public rightly expects that the use of such capabilities will be subject to clear justification, robust oversight and meaningful redress in the event of error or harm. This document provides guidance through which those expectations can be consistently and credibly met.

As with previous innovations such as biometrics, body-worn video and breathalyser technologies, UK policing has a proven track record of integrating new tools in a manner that respects legal, ethical and societal norms. However, the scale, adaptability and potential for expansion inherent in AI demand an enhanced approach. Without appropriate safeguards, the risk of unintended consequences and mission creep is significant.

This guidance supports policing organisations in addressing those risks through foresight, planning and institutional readiness. It reinforces the principle that advanced technological capability must be matched by advanced accountability measures. In doing so, it aims to sustain the legitimacy of policing in a democratic society, ensuring that public trust is not only maintained but strengthened in the face of technological change.

Prof Babak Akhgar OBE
Director of CENTRIC

Prof John Parkinson OBE
Chair of CENTRIC Board

Table of Contents

03 Foreword

07 Purpose of the guidance

08 AI accountability: What, why and how?

10 Conceptual foundation for the guidance

13 Translation into eight practical themes

14 How to use this guidance

15 Guidance and themes

52 Appendix A: Core accountability stakeholders

54 Appendix B: Lifecycle legislative considerations

55 Appendix C: Glossary

56 Bibliography

57 Methodology

Purpose of the guidance

This document provides **concise, step-by-step guidance on how to implement AI accountability** for police Chief Officer Teams, Enabling Services involved in the procurement and deployment of AI systems and oversight bodies. The guidance lays out **considerations, safeguards and resources to put into place for a comprehensive risk assessment and risk management for AI in UK policing.**

The guidance is organised along eight themes that ensure that the AI system, its purpose, data, and impacts, as well as related oversight and redress procedures can be assessed and managed in a comprehensive manner.

We further offer AI accountability considerations for each distinct period in the AI lifecycle – namely, design/procurement, deployment and migration/decommissioning – as well as for distinct roles with AI accountability responsibilities.

The **core objectives of this guidance** are to:

- Provide a **comprehensive risk assessment and management approach** for the adoption of AI into policing
- Aid policing to **proactively plan and put in place resources, procedures and safeguards** to ensure the responsible and accountable procurement and use of AI
- Assist **oversight bodies to assess and review AI decisions and arrangements**
- **Support policing in evidencing** that it is acting responsibly and accountably towards the public
- **Demonstrate transparency** in the usage of AI in line with national requirements

Intended users

- Chief Officers
- AI Users
  - Operational or business users/deployers
  - Managers with responsibilities for AI procurement and deployment
  - Enabling Services (e.g., data protection professionals and legal services)
- Policing Oversight Bodies

Additional interest groups may include AI developers seeking insight into requirements for the policing domain. The guidance may also be of use to those creating Standard Operating Procedures (SOP), engaging in IT progression or organisational development planning, corporate communications and training development.

AI accountability: What, why and how?

What we mean by accountability: Accountability is the acknowledgement of an organisation's responsibility to act in accordance with the legitimate expectations of stakeholders and the acceptance of the consequences – legal or otherwise – if they fail to do so. [i]

AI in policing and the importance of accountability

Accountability is about people with power using it properly. Where those people are the police, their use of power can have profound consequences. If their power is amplified by technology, accountability extends to its use. **In a policing model based on consent, advanced technology must come with advanced accountability.**

As AI comes to policing, it will therefore bring greater complexity in accountability mechanisms that will differ in some respects from other sectors. All public bodies need to use technology, and they all need to respond to questions like 'what exactly does it do and why do you need it?' People also want to know what happens if it goes wrong and where can they find out more about it. This is 'entry level' answerability, where policing is no different from any other public service – they must provide answers to questions about their use of tech-enabled capabilities.

AI presents policing with different, more demanding, accountability requirements. If they are using elemental 'narrow' AI for purely administrative functions, the police will have the same level of accountability as other public bodies, but using an AI capability to support operational policing functions would be a wholly different use case. Where AI-enabled technology is being used for a law enforcement purpose such as remote biometric identification and covert surveillance, policing should anticipate deeper levels of accountability. And when using inferential algorithms that calculate age, mood or race, the stakes are much higher whoever is using it, and all sectors will need to reflect the legal refinements and reinforce the necessary safeguards.

UK policing has a strong record of embracing accountability when adopting innovative technology. Biometrics, breathalysers and body worn video are examples. Two things make AI different: novelty and capacity. Being endlessly multi-functional, AI-enabled capability is very likely to go beyond its original brief and, with technology in an almost perpetual beta state, AI will offer ever wider applications as a constant. This is one of AI's strengths; it is also the basis of 'mission creep' which needs to be guarded against.

The National Police Chiefs' Council (NPCC) Covenant for using AI in Policing[ii] is focused on a number of requirements that policing organisations should follow in procuring, developing and introducing AI-enabled tools. The national Digital Science and Technology strategies recognise: (1) the power of algorithms to achieve a 'step change' in policing efficiency, (2) the 'arms race' with criminals exploiting new technologies and (3) the need to maintain public confidence through standards, an ethical framework and independent oversight.

The NPCC Covenant is built on several generic principles for AI, such as compliance with applicable laws, standards and regulations, 'Maximum Transparency by Default' (MTbD) and protocols that allow a third-party to investigate the algorithmic workings, scenarios and data from an 'adversarial perspective', and also the ability for any AI to provide an 'explanation' of its output.

All AI that affects the public must have responsible usage policies and procedures to ensure that users do not accept AI outputs uncritically. Further, all AI that affects the public must have a human as the ultimate decision-maker, together with human or automatic means of being stopped if it displays unintended or undesired outputs and proactive mitigation of risk from unintended biases or harms at all stages. All of these features are incorporated within and directly supported by this guidance.

The Government Office for Artificial Intelligence's Guidelines for AI Procurement[iii] further informs contract implementation and management. The use of AI in policing must comply with established codes of practice including the College of Policing's Code of Ethics,[iv] which describes the standards of accountability, fairness, honesty, integrity, leadership, objectivity, openness, respect and selflessness that is expected of all in policing. **This guidance addresses these areas in practical detail and provides a tool for self-audit to ensure compliance and continuous best practice.**

The direction of travel is towards principles embedded not only in policy, but also in practice. As AI systems become more deeply entwined with public facing policing activities, unique challenges for accountability will arise. **This means policing organisations must progress beyond minimum compliance checklists.** Policing must demonstrate adaptive practices with meaningful oversight, robust internal governance and effective independent scrutiny. Open and routine public engagement and transparent audit trails are critical in this dynamic technology environment.

All of these ideas must be operationalised, to ensure the public can trust that the police's AI use is not only efficient and effective, but also justified and proportionate. **This guidance focuses on this important fact, and helps policing organisations putting AI into practice.**

Benefits of implementing AI accountability

What we mean by AI accountability: AI accountability ensures that policing organisations have evidence of their infrastructures, resources, risks, decisions, etc., as well as clear, agreed procedures how to react to and redress failures (i.e., address both proactive and reactive accountability).[v]

Done well, AI accountability is a highly practical instrument, as it helps to think through the why, what, how, who and for whom of AI deployments. Implementing AI accountability can ensure that adequate practices and infrastructures are set up before things go wrong (i.e., aiming to prevent failures) and if they go wrong, people know how to respond.

Implementing AI accountability is therefore proactive risk assessment and risk management.

Benefits of AI accountability[vi]

- Understand the risks and strengths before each AI procurement, deployment or change
- Know up-front what to do if something goes wrong
- Understand which areas of AI accountability are achieved or need addressing
- Have evidence ready in case of challenges and requests to prove adequate AI procedures

Conceptual foundation for the guidance

The conceptual foundation of this guidance are **twelve AI accountability principles**, which were developed with police practitioners and legal, ethics and industry experts.[vii]

These principles form the basis on which to assess and evidence the responsible and accountable usage of AI in UK Policing.

Detailed description

Lawfulness - Follow the law

All aspects of the use of AI should be lawful. The burden of proving that they are, sits with the user. It may seem obvious but the starting point for AI accountability requires compliance with international, national and local laws. Lawfulness includes compliance with specific legal requirements and also includes your organisational policies, which must be clearly identified and readily available. Lawfulness applies in every situation but is not the only form of AI accountability in policing and law enforcement. In some ways, the rest of the Principles are Lawfulness Plus.

Completeness - Leave nothing out

AI accountability arrangements must cover all relevant aspects of AI deployments, including partners and sub-contractors. This Principle effectively extends the reach of AI accountability arrangements and reflects the fact that AI applications are necessarily multi-partner input programmes. Public trust and confidence must extend to the whole AI ecosystem including design, development and supply. Where there are any gaps in the AI accountability arrangements (such as areas not expressly covered by the law), the protection and promotion of fundamental rights and freedoms should prevail.

Transparency - Be open

AI accountability needs clear, accurate and meaningful information. This Principle is intended to ensure such information about AI systems is available (subject to operational sensitivities); it is also about the overall AI accountability arrangements. Information should establish the necessity and proportionality of use of AI systems and highlight foreseeable risks. This Principle aims to promote public trust and confidence by enabling those directly and indirectly affected to make informed judgments and risk assessments about the use of an AI system and the AI accountability arrangements.

Proof - Follow the evidence

Law enforcement bodies are very familiar with capturing, analysing and presenting relevant, reliable evidence. AI accountability requires a forensic approach to all aspects of AI systems and of the accountability process itself, demanding and following clear evidence. The quality of that evidence should reflect the potential impact of the AI system's use/non-use and mirror the standards of operational evidence gathering in terms of integrity, credibility and continuity.

Inclusivity - Leave no one out

Oversight must involve all relevant stakeholders engaged in and affected by a specific AI system or deployment. The Principle of Inclusivity builds in diversity and reduces the risk of bias (actual or perceived), where everyone regulating the AI system seems to come from the same background as those who are using it. Inclusivity can be achieved by having broad participation of stakeholders in creating policy, reviewing deployment and looking for learning points.

Explainability - Describe, demonstrate, demystify

Those using AI systems need to provide information about it in a meaningful way that is easily understood by the relevant participants/audience. Being able to explain the AI system in a technical and legal setting is one part of this Principle. A harder challenge is being able to explain it more generally in non-technical language so that the citizen and their representatives can understand, participate and challenge the use of AI. As with Compellability, requirements for a basic level of explainability might be written into contractual agreements with designers, providers and partners.

Compellability - Make it work

Closely linked to Enforceability and Redress, this Principle means oversight bodies must be in position to make the AI accountability arrangements work. External compellability will usually come from legal or democratic frameworks, while internal frameworks should authorise the provision of necessary information and access by creating formal obligations and without the need to deploy external legal powers. For example, there should be mechanisms to access the necessary information about the deployment and functioning of AI systems. Policies should give relevant bodies the ability to compel the sharing of necessary information and evidence required under some of the other Principles without having to invoke the legal powers of courts and tribunals.

The timely provision of relevant, up to date and accurate information in an intelligible format contributes to the AI accountability process. Linked closely with Enforceability and Redress, this Principle will be supported by contracts and Data Sharing Agreements.

Impartiality - Empower independence

AI accountability bodies need to be impartial and independent without any conflict of interest. For external accountability paths – such as courts and regulators – this is usually built in. Complete independence internally is almost impossible, as many key decision makers will be from the same organisations. Wherever practicable, individuals and organisations involved in the AI accountability mechanisms for AI systems should have a degree of independence from the line management structure of those involved in their design, procurement, supply and deployment. This applies in a personal, political, financial and functional way. Any conflict of interest must be identified and addressed.

Learning - Look for the lesson

This Principle promotes the willingness of organisations and people to improve AI in every respect through the application of (new) knowledge and insights. It applies to everyone and everything involved in the design, use and oversight of AI in the policing domain (security practitioners and partners, industry, oversight bodies, etc.). Learning includes the modification and improvement of systems, structures, practices, processes, knowledge and resources, as well as the development of professional doctrine and agreed standards.

Enforceability and Redress - Make it right

Without a 'so what?' element, AI accountability will be heavily diluted. For it to be meaningful to stakeholders, AI accountability must be underpinned by mechanisms giving people an effective remedy. These will include external legal and procedural routes for complaint and challenge; but also internal mechanisms for individual enforceability and redress (such as professional and policy standards) and contractual arrangements are vital. Enforceability and Redress is closely linked to the Lawfulness Principle and can be achieved via national regulators. However, the ability of oversight bodies to intervene, to require policy reviews and to publish findings are also an important part of AI accountability.

Constructiveness - Aim for better

AI accountability is more than criticism. This Principle means that all stakeholders participate constructively with a shared aim of improvement. This may include considering different perspectives, inviting challenge and recognising how disagreement can lead to beneficial solutions. Constructive accountability will be needed to build trust and confidence in the use of AI, internally and externally.

Conduct - Hold yourself accountable

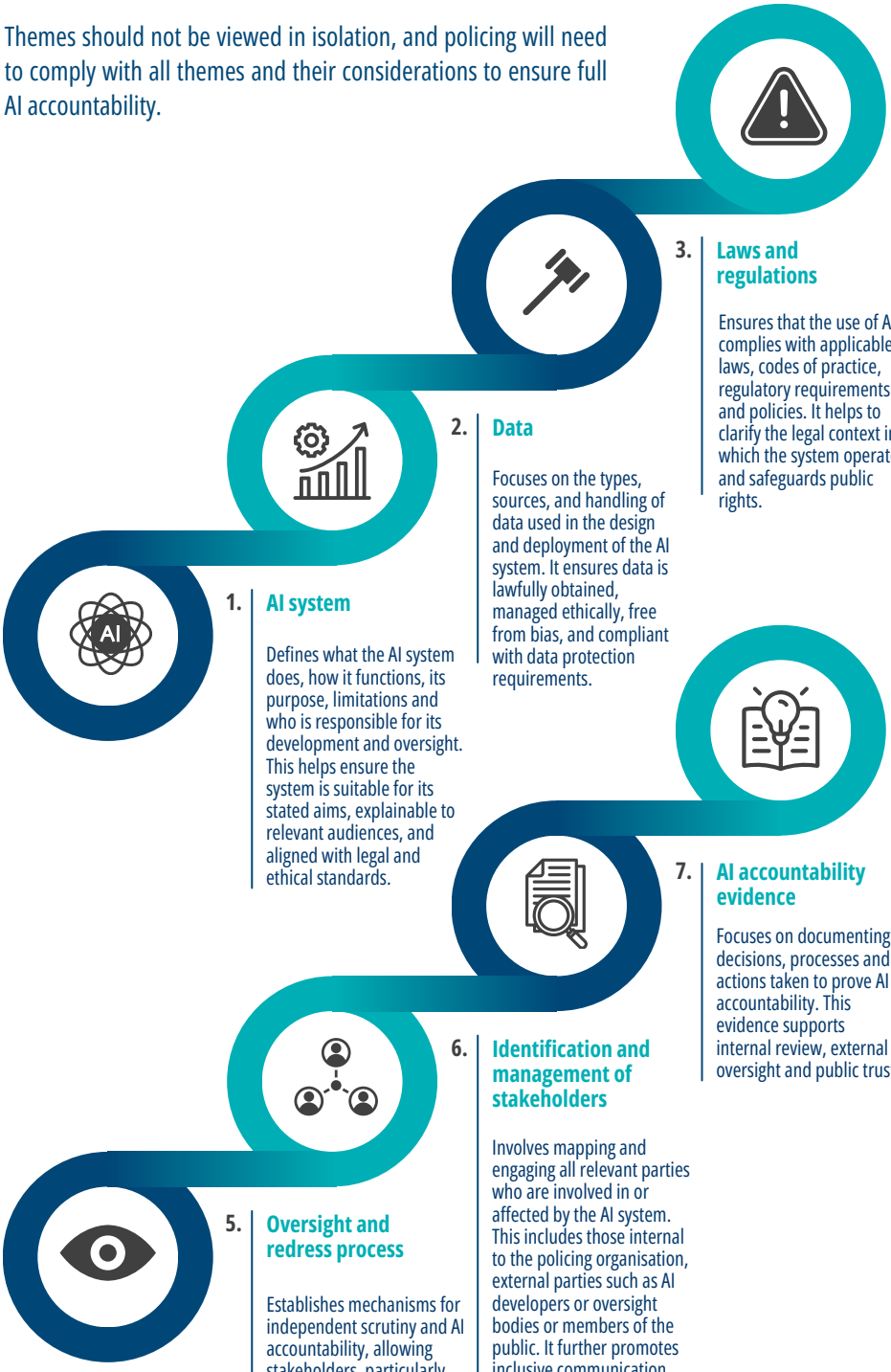
The conduct of policing will increasingly include the use of AI technology, and this Principle is both individual and organisational. It relates to professional standards, values and expected behaviours which incorporate integrity and ethics. This Principle extends the formal responsibilities to an AI context, where adherence to agreed AI-specific standards is of crucial importance to trust and confidence. Where partners using the AI system are from different jurisdictions, with different legal systems and cultures, there may be a requirement for closer scrutiny and review mechanisms. The approach may vary according to the agency involved, ranging from internal complaints handling, dispute resolution and mediation frameworks, to formal professional proceedings before courts or tribunals.

Translation into eight practical themes

The guidance uses eight themes to support the implementation of the AI accountability principles. **The eight themes capture core areas in which potential risks can emerge to the legitimacy of AI capabilities, their usage and/or the police organisation**. The themes make the 12 AI accountability principles practical and implementable.

The themes break down AI accountability into manageable sections that can be operationalised, so policing can develop robust, practicable mechanisms and processes to safeguard itself, its users and the public.

Themes should not be viewed in isolation, and policing will need to comply with all themes and their considerations to ensure full AI accountability.



1. **AI system**

Defines what the AI system does, how it functions, its purpose, limitations and who is responsible for its development and oversight. This helps ensure the system is suitable for its stated aims, explainable to relevant audiences, and aligned with legal and ethical standards.

2. **Data**

Focuses on the types, sources, and handling of data used in the design and deployment of the AI system. It ensures data is lawfully obtained, managed ethically, free from bias, and compliant with data protection requirements.

3. **Laws and regulations**

Ensures that the use of AI complies with applicable laws, codes of practice, regulatory requirements and policies. It helps to clarify the legal context in which the system operates and safeguards public rights.

4. **Risk assessment and management**

Identifies risks, harms or biases associated with the AI system and implements mitigation measures. It covers both the impact of using and not using AI, with an emphasis on fairness and public safety.

5. **Oversight and redress process**

Establishes mechanisms for independent scrutiny and AI accountability, allowing stakeholders, particularly the public, to challenge decisions and seek corrections; ensuring just outcomes.

6. **Identification and management of stakeholders**

Involves mapping and engaging all relevant parties who are involved in or affected by the AI system. This includes those internal to the policing organisation, external parties such as AI developers or oversight bodies or members of the public. It further promotes inclusive communication, engagement and trust-building.

7. **AI accountability evidence**

Focuses on documenting decisions, processes and actions taken to prove AI accountability. This evidence supports internal review, external oversight and public trust.

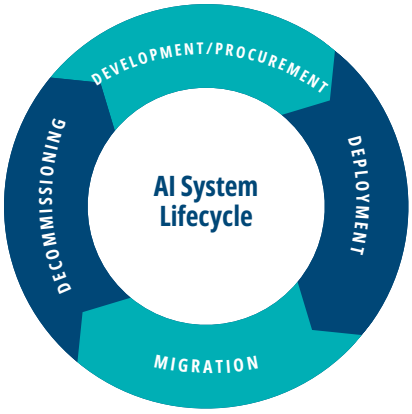
8. **Adaptability and learning**

Encourages continuous improvement through feedback, review and learning. Ensures the AI system and its use evolve responsibly with new insights, legal updates and societal expectations.

How to use this guidance

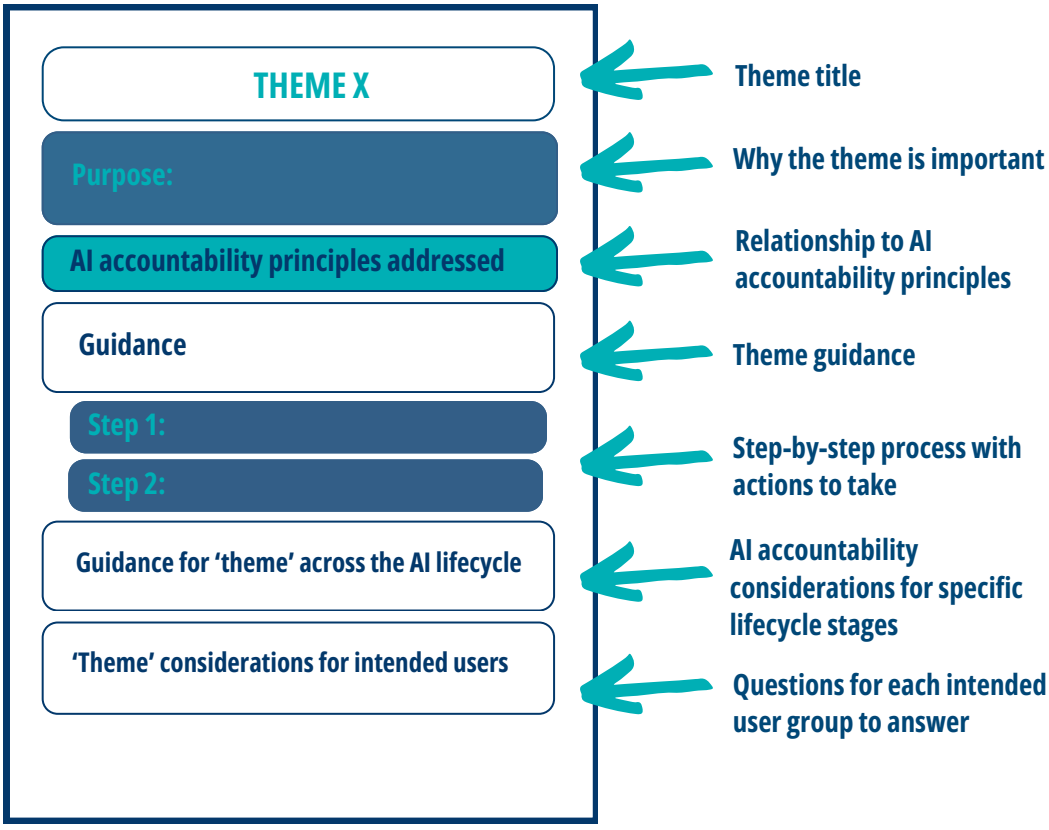
This guidance should be **used as a practical tool to assess and prepare for AI accountability across all stages of an AI system's lifecycle.**

- **Development/Procurement:** Creating or acquiring an AI system, including data preparation, model design and ethical/legal evaluation
- **Deployment:** Integrating the AI into organisational use, with monitoring and oversight to ensure safe and effective operation
- **Migration:** Updating, adapting or relocating the AI system to new contexts while maintaining reliability and compliance
- **Decommissioning:** Safely retiring the AI system, preserving necessary records and mitigating disruption or residual risks



The guide acts as a reference point that will ensure policing organisations capture key AI accountability considerations and requirements throughout the AI system lifecycle.

To manage this, the guide is divided along the eight practical themes. Each theme provides concrete steps for implementation, including actions and considerations during their implementation. They are complemented by AI accountability responsibilities along AI lifecycle phases: procurement/development, deployment and migration/decommissioning. This is followed by considerations for the three core user groups of this guidance: Chief Officers, AI Users and Oversight Bodies. These are nominally displayed as questions, enabling users to consider requirements to demonstrate AI accountability responsibilities and thus AI accountability. The relevant AI accountability principles are stated at the beginning of the theme to indicate which principles are addressed within the theme.



Guidance

16 Theme 1: AI System

20 Theme 2: Data

25 Theme 3: Laws and Regulations

28 Theme 4: Risk Assessment and Management

34 Theme 5: Oversight and Redress

40 Theme 6: Identification and Management of Stakeholders

45 Theme 7: AI Accountability Evidence

49 Theme 8: Adaptability and Learning

Theme 1: AI System

Purpose: This theme defines what the AI system does, how it functions, its purpose, limitations and who is responsible for its development and oversight. This helps ensure the system is suitable for its stated aims, explainable to relevant audiences, and aligned with legal and ethical standards. The better a police organisation details the AI system, the more effectively itcan assess its appropriateness, identify potential challenges and implement safeguards.

AI Accountability Principles addressed: Lawfulness, Proof, Completeness, Explainability, Transparency, Enforceability and Redress

Guidance

Need, requirements and features

Step 1: Understand the need for the AI system

It is important **to set out the need for a specific AI system and justify why it is the appropriate solution** compared to conventional methods or other AI systems.

Much of the information that demonstrates the need would sit within a business case, and each AI system that is being developed, procured or deployed will require its own justification. In identifying the need, a force will start to shape the requirements of the AI system, which can be fed into a development, procurement, deployment or decommissioning strategy. Where possible, principles such as JAPAN (Justified, Accountable, Proportionate, Auditable, Necessary) should be applied.

Step 2: Identify the requirements and features of the AI system

Each AI system will have different requirements and features based on the identified need for the AI system, so it is important that these are carefully considered and documented.

A policing organisation should, at the very minimum, have a record of:

- How the AI system will be used (purpose and implementation)
- The AI system's functionalities and features, including its models/algorithms

A policing organisation must also consider its **own IT requirements such as ISO accreditations and cybersecurity certifications** and how these standards apply or impact the procurement/use of the AI system.

The record of requirements also needs to include features that can display how an AI system comes to a certain output. This is particularly important if the output is used as part of an evidential chain.

A policing organisation needs to be able to demonstrate:

- The process by which the AI system reaches a decision
- How decisions of the AI system are documented
- How/whether the AI system's outputs can be overridden, e.g.,
  - Is it possible to circumvent decisions made by the AI system?
  - Will the AI system have a human or automatic means of being stopped if it displays unintended or undesired outputs?
  - Are wrong decisions or outcomes by the AI system fully reversible?

Step 3: Identify responsible parties involved with the AI system

A policing organisation needs processes and mechanisms to manage the AI system. **Understanding early how these processes and mechanisms look like and who is responsible for them** will help design a practical and effective AI ecosystem.

For this, a policing organisation will need to understand and have a record of:

- The processes and related responsibilities for the AI system's design/procurement (including feature selection), deployment, modification, migration and decommissioning
- The 'Maximum Transparency by Default' (MTbD) requirement and how it will be managed

Maximum Transparency by Default (MTbD) is an open government policy stance. It proposes that public sector entities proactively disclose information to the greatest extent possible, unless there is a compelling and clearly justified reason for confidentiality (e.g., operational security, public safety, personal privacy). This creates an organisational assumption of openness and places a burden of proof to demonstrate why any information should be withheld.[viii]

AI System considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Problem Definition and Justification:** Clearly set out the specific problem or operational gap the AI system is intended to address and justify why this AI solution is more appropriate than conventional methods or other AI solutions
- **Functionality Documentation:** Record the AI system's core functionalities and the rationale behind them
- **Operational Use Definition:** Define how the system is to be used within operational contexts
- **Third-Party Involvement:** Identify and document third-party involvement, including obligations for training, maintenance and support
- **Legal and Policy Compliance:** Ensure that the procurement process complies with relevant legislation and organisational policy
- **Contractual Requirements:** Confirm that procurement contracts include necessary clauses, ensuring required support over the system lifecycle. This includes continued support relating to technical aspects of:
  - Legal compliance
  - Data protection
  - System maintenance
  - Monitoring and updates
  - Audit and inspection
  - Intellectual property and access
  - Termination and exit
- **Exit Strategy:** Include an exit strategy into contractual agreements
- **Responsibility Assignment:** Identify and record who is responsible for:
  - The design of the system
  - Procurement
  - Deployment and operation
  - Support and maintenance
  - Modification
  - Migration
  - Decommissioning
- **Procurement Accountability:** Include checks that ensure decisions made during procurement are transparent and can be audited
- **Documentation Accessibility:** Ensure documentation is available for internal and external scrutiny, and that procurement decisions can be explained to oversight bodies or the public, if needed

AI Accountability responsibilities during deployment

- **Purpose Alignment:** Ensure the AI system is deployed in line with its documented purpose
- **Decision Record Keeping:** Maintain clear records of decisions made based on AI inputs/outputs
- **Ongoing Review:** Continually review the AI system and the wider AI ecosystem for intended and unintended results of the deployment
- **Feedback Mechanisms:** Ensure feedback processes are available, specifically on continued fit-for-purpose, quality and impacts
- **Learning mechanisms:** Ensure procedures are in place that allow modifications to the AI system and/or its usage, if issues are identified
- **Redress Mechanisms:** Ensure procedures are in place that provide effective redress and remedies

AI Accountability responsibilities for migration/decommissioning

- **Decision Transparency:** Document clearly the need and rationale for the migration/decommissioning decision
- **Transition Planning:** Develop and follow a transition plan to ensure continuity of service for ongoing functions or investigations
- **Data and Outcome Archiving:** Archive key data and outcomes from the AI system, in a format with proven longevity and long-term accessibility and in line with data protection requirements
- **Documentation Archiving:** Archive key documentation (e.g., decision logs, procurement/deployment records) in a format with proven longevity and long-term accessibility
- **Access Right Maintenance:** Ensure appropriate access rights to documents and that data are maintained (e.g., when archives are moved or staff are leaving/changing roles)

AI System considerations for intended users

Chief Officers

- **Necessity and Proportionality:** Do you have a demonstrable need for the AI system, including possible outcomes if not using the AI system?
- **Forward Planning:** Does your organisation have a procurement, deployment, migration/decommissioning plan?
- **Specification Development:** Has an end-to-end user requirement specification document been produced?
- **Logs and Record Keeping:** Have all relevant decisions been recorded and explained in a way that is understandable to the intended audience?
- **Data Sources:** How do you ensure that data used by the AI system is appropriate, including free of bias?
- **Fairness and Optimisation:** How do you ensure the AI system and data used are unbiased or, if not possible, biases are identified and mitigated?

AI Users

- **Technical Practicality:** Can the current IT infrastructure support the AI system?
- **Accountability Awareness:** Are you aware of your responsibilities with respect to AI accountability?
- **Information and Accessibility:** Do you know where to seek guidance on the AI system and AI accountability requirements?
- **Operational Context (design):** Is the AI system used in the settings and circumstances for which it was designed?
- **Operational Context (authorisation):** Is the AI system being used within the settings and circumstances which have been authorised by your policing organisation?
- **Monitoring:** Do you have the means to monitor the performance of the AI system to check it remains in line with its intended purpose and quality requirements?
- **Intervention Protocols:** Do you know when and how to overrule AI decisions or recommendations, and when to escalate concerns regarding system behaviour?
- **Training Requirements:** Have you all the necessary information to carry out your task with the AI system?
- **Training:** Have you received sufficient training to be authorised to use this system and operate it lawfully?
- **Audit Trail:** Are your decisions for AI input/outputs or decisions based on AI inputs/outputs adequately recorded?
- **Mitigation Strategy:** Are appropriate measures in place to mitigate the impact of residual data or algorithmic bias?
- **Update and Modification Strategy:** Do you have a clear strategy for when and how to process updates or modifications?

Oversight Bodies

- **Compliance and Objective Alignment:** Does the AI system, its requirements and functionality achieve their stated purpose lawfully and effectively?
- **Ethical Governance Planning:** Are there any foreseeable ethical issues that may arise from using the AI system, and has a solution/mitigation roadmap been created?
- **Ongoing Assessment and Best Practice Guidance:** Are you monitoring and reviewing the AI system's lifecycle?

Theme 2: Data

Purpose: This theme establishes an understanding of the data involved in creating the AI system (training/test data), as well as the data created for and by the AI system (inputs/outputs). It further ensures clarity about data management, risks and regulations, focusing on a number of critical considerations:

- Detailing the types and sources of data used in the development and deployment of the AI system, allowing proper evaluation
- Establishing transparent procedures for lawful and appropriate acquisition, processing and management of data
- Ensuring that legislative and policy compliance procedures in relation to data are effectively implemented and documented
- Confirming the roles of responsible actors in relation to data are established, they are aware of their responsibility and possess appropriate skills and knowledge

AI Accountability Principles addressed: Lawfulness, Proof, Completeness, Inclusivity, Explainability, Transparency, Enforceability and Redress, Impartiality, Conduct, Learning

Guidance

Types and sources of data

Step 1: Detail the types and sources of data

Understanding the source and nature of data used in the development of the AI system, as well as the data used by and produced by the AI system is an important step in an informed assessment of the system and its outputs and impacts.

To accomplish this, there should be a comprehensive record of:

- The data used in the development of the AI system
- Data used and generated by the AI system
- Information on data relating to marginalised or vulnerable groups

Awareness of data biases: "As AI systems learn from data which may be unbalanced and/or reflect discrimination, they may produce outputs which have discriminatory effects on people based on their gender, race, age, health, religion, disability, sexual orientation or other characteristics." (Information Commissioner's Office, 2023)[ix]

To ensure accurate and consistent outputs it should be confirmed that:

- Any bias present is known and documented
- Appropriate mitigation measures against bias are in place where required
- There is appropriate statistical weighting and validity for all data subjects

These measures aim to establish a baseline of functionality for all individuals subject to the system.

Step 2: Know the requirements for personal data

The standard outlined by UK GDPR, including completion of a DPIA, remains relevant throughout the lifecycle of the AI system. It should be confirmed **whether the AI system processes sensitive or personal data at any stage of its lifecycle.**

If so, the organisation should confirm:

- The necessity and proportionality of all processing of personal data
- The presence of procedures to inspect and control the processing of personal data
- Systemic human intervention in the processing of personal data
- Compliance of the AI system's processing of personal data with retention policies

Data acquisition and management

Step 3: Set up clear data collection and processing protocols

An important element for AI accountability is the **ability to justify the provenance and processing of data for and within the AI system.**

This includes data

- Used in training, validation and testing of the AI system
- Input data used by the AI system
- Any data acquired from a third party or re-purposed from existing data sets

In developing protocols and documentation about the acquisition and processing steps, it should be considered how the data was:

Chosen | **Designed** | **Collected** | **Prepared**

Preparation may include annotations, labelling and cleaning of data.

Each of the activities above represents a point of risk for the introduction of bias. An overview how each process takes place allows confirmation of compliance with relevant standards both before and following the procurement of the AI system.

Data governance

Step 4: Assurance of relevant legislation and policy in the context of AI data

It should be confirmed that existing data governance processes within the organisation encompass the use of AI systems.

Standard requirements include:

- Assurance of UK GDPR compliance
- Completion of a DPIA, with regular updates
- Appropriate Data Protection Policy

These established practices should be assessed to confirm that internal policy is suitable for the use of the AI system. It may be the case that the existing policy is already appropriate. However, this evaluation and the grounds for it should be recorded. Where AI systems were developed before procurement, it should be confirmed that data protection compliance was built into the system design.

Step 5: Ensure continued compliance with obligations for all data processors

Written agreements should be signed to ensure all relevant data processors are aware of their commitments. This ensures that all parties are aware of their obligations. In the case of external parties, written contracts may also guard against the withdrawal of critical updates or data protection functions.

As with any IT system, building and maintaining compliance to adequate data practices is a core challenge. **In this respect, overarching knowledge and training requirements are:**

- Data protection awareness for all staff
- Specific training for the AI system end-users/other accountable individuals
- Integration within training of how to identify and report a personal data breach

However, training alone is not sufficient. **To maintain compliance and ensure adaptation of data practices, there should be a regular review of:**

- Continued compliance with data protection policy and regulations
- Effectiveness of data handling
- Proper functioning of security controls, including cybersecurity
- Effectiveness of the reporting and mitigation processes for data breaches

Data considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Legality:** Ensure compliance with UK GDPR, the Equality Act 2010, ethical standards and other relevant requirements for data protection
- **Data Sources and Compliance:** Conduct due diligence on those providing or developing the AI system and AI models (including data sources, bias mitigation, model transparency)
- **System Maintenance:** Include clear contractual obligations for continued system maintenance, where applicable (e.g., security, updates, audit access)
- **Risk Management:** Document intended use, risks and safeguards for all types of data, with special focus on personal and sensitive data
- **Consultation:** Engage DPOs, legal and operational leads early; consult externally if data acquisition/processing is high-impact or otherwise a matter of public interest

AI Accountability responsibilities during deployment

- **Oversight Responsibility:** Assign clear points of accountability for data oversight
- **Access and Data Rights:** Set up clear responsibilities and rights for data accessing, processing, modification, deletion, etc.
- **Accuracy and Impact:** Monitor for bias, accuracy and disproportionate impacts of data practices, particularly for protected groups
- **Data Protection:** Follow data handling, security and breach response laws and policies
- **Security Protocols:** Establish clear protocols for handling data misuse and breaches from actions with or of the AI system, including reporting, mitigation and redress of the misuse/breach
- **Learning:** Provide regular training and maintain audit-ready documentation on data practices and data management

AI Accountability responsibilities for migration/decommissioning

- **Compliance:** Ensure that the discontinuation of the AI system complies with all existing data retention, deletion and data subject rights under UK GDPR
- **Preservation:** Review whether any ongoing legal or public interest obligations require preservation of certain datasets or system outputs
- **Data Storage**: Establish who has control to remaining/retained data, where it is located and how it can be accessed
- **Archiving:** Archive necessary records for AI accountability and transparency, in a format proven to ensure longevity of data access
- **Record Keeping:** Document reasons for retention or deletion of datasets
- **Completeness:** Ensure third parties also remove stored data, where applicable
- **Final Review:** Conduct a lessons-learned review of data practices to inform future AI procurements/use

Data considerations for intended users

Chief Officers

- **Strategic Accountability:** Are monitoring structures in place to ensure responsible data use and publication, in line with legal and ethical standards?
- **Lawfulness Assurance:** Are you confident that the planned processing of personal and sensitive data is lawful, especially when systems repurpose legacy data?
- **Governance Integration:** Do you have assurance that AI-specific requirements are incorporated into existing data governance structures, risk assessments and policies (e.g., UK GDPR, Equality Act 2010)?
- **Oversight of Development:** Are you confident that all data sources used in system development are known (including those from third parties)?
- **Bias and Fairness:** Do you have evidence that data bias has been adequately identified, assessed and mitigated against, particularly concerning vulnerable and marginalised groups?
- **Public Assurance:** Is the information about how the AI system uses data sufficiently available and suitable for public communications and community assurance?

AI Users

- **Data Protection:** Are you aware of how data protection requirements interact with the operation of the AI system?
- **Data Integrity:** Has all critical information been inputted into the AI system, allowing complete and honest outputs?
  Awareness of Limitations: Are you aware of any limitations or biases from training data and/or algorithms, which may affect the system?
- **Bias Vigilance:** Do data and accepted use policies ensure users remain alert to potential signs of erroneous or discriminatory outcomes, especially regarding protected characteristics?
- **Personal Data Handling:** Are procedures in place to ensure that all interactions with personal or sensitive data are lawful, necessary and proportionate?
- **Documentation Requirements:** Are you aware of requirements for record keeping in relation to data acquisition, processing, access and storage and grounds for decision-making?
- **Incident Reporting:** Do you know the correct method to report data protection breaches or unusual system outputs?
- **Training Compliance:** Have you received sufficient and required training on correct and safe data practices, including refresher training to remain certified?

Oversight Bodies

- **Audit Trails:** Do comprehensive records exist for all data used in the AI development and deployment, including third-party and legacy datasets?
- **Bias Detection Processes:** Are methods for identifying and mitigating bias in place, ensuring considerations for inclusion of minority/vulnerable groups?
- **Validation Evidence:** Is there sufficient statistical validity, weighting and test outcomes for AI models, particularly regarding fairness and generalisability?
- **UK GDPR and DPIA Oversight:** Is data protection compliance adequate and complete, particularly considering sensitive data use and system changes/evolution?
- **Compliance Monitoring:** Are regular internal reviews conducted on data handling, system updates and breach management?
- **Policy Adequacy:** Do internal policies sufficiently address AI-specific data risks and are they followed in practice?
- **Third-Party Accountability:** Has the policing organisation ensured external vendors comply with contractual obligations on data protection and system integrity?
- **Transparency and Publication:** Are there clear standards for documenting and, where appropriate, publishing information about AI data processes, consistent with national best practices?
- **Continuous Improvement:** Are procedures in place to ensure that improvements are an integral part of the review process, based on observed issues or evolving standards, including technological updates and procedural reforms?

Theme 3: Laws and Regulations

Purpose: Lawfulness is an overarching principle in all areas of AI accountability. It ensures that the use of AI complies with applicable laws, codes of practice, regulatory requirements and policies. It further helps to clarify the legal context in which the system operates and safeguards public rights.

AI Accountability Principles addressed: Lawfulness, Proof, Completeness, Explainability, Enforceability and Redress, Conduct

Guidance

Legal obligations

Step 1: Understand which laws apply to the AI system and current lifecycle stage

A policing organisation must fully understand which laws, regulations and policies apply to the specific AI system, its purpose and application context.

For this purpose, a policing organisation must:

- Identify all applicable laws, regulations and policies for the designing/procurement, deployment and migration/decommissioning of the AI system, including any legal exemptions granted or safeguards enforced
- Ensure the use of the AI system is necessary and proportionate for the given purpose (see Example)
- Ensure relevant entries are recorded in the National Record of Processing Activities

Different AI systems and application contexts will trigger different legal requirements. For example, an AI system managing a vehicle fleet will be subject to different regulatory frameworks than a system used for facial recognition. To assist in identifying relevant legislation, an illustrative table is provided in Appendix B, highlighting a non-exhaustive list of laws and regulations.

Where there is no AI/purpose-specific law present, a policing organisation should still follow existing legal frameworks and align with national guidance and local policy.

When **working with international partners**, a policing organisation needs to be aware of, and possibly follow, other AI legal frameworks and regulations (such as the EU AI Act when working with agencies within Europe).

Example - Breach of data protection laws[x]

Under the Data Protection Act 1998, the Information Commissioner's Office (ICO) issued an Enforcement Notice to the Metropolitan Police Service (MPS) concerning its use of the Gang Violence Matrix (GVM), a tool designed to identify and assess the risk posed by individuals involved in gang-related violence across London. While the ICO acknowledged that the database served a legitimate purpose, it found that its application was unlawful and extended beyond what was necessary. As a result of the investigation, hundreds of individuals were removed from the matrix, and the GVM was eventually decommissioned by the MPS.

Step 2: Put procedures in place that monitor compliance with laws and regulations

Once the applicable laws and regulations are identified, the policing organisation must take proactive steps to ensure compliance throughout the AI system's lifecycle. Each AI system may require a tailored compliance approach, depending on its purpose, impact and data used.

To support monitoring of legal compliance policing should:

- Ingrain laws and regulations that govern the AI system into monitoring and review procedures
- Remain abreast of changes in the law and/or regulatory requirements
- Conduct reviews of the AI system and its usage, when new laws and/or regulatory requirements are enforced

Laws and Regulations considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Legal Compliance:** Document all applicable laws, regulations, policies and potential exemptions for the system's intended use
- **Expert Review:** Ensure the AI system has been reviewed by a competent legal professional, to ensure compliance with relevant legislation
- **Necessity and Proportionality:** Evidence that the AI use is both necessary and proportionate for its stated purpose
- **Public Record:** Ensure the AI system is logged appropriately in the National Record of Processing Activities
- **Alignment with Existing Standards:** Confirm alignment with internal and external governance frameworks (including national guidance, Codes of Practice and local policies)
- **Provider Disclosure:** Require external system providers to provide a full disclosure of data sources and system functionalities
- **Provider Accountability:** Ensure third-party providers can demonstrate that the AI system has been developed in a lawful way and does not contravene Codes of Conduct, ethics or any other policing guides and regulations
- **Contractual Obligations:** Include legal compliance obligations and access to internal system documentation in provider contracts

AI Accountability responsibilities during deployment

- **Designated System Owner:** The system sponsor is aware of their responsibility for system use, outputs, oversight and adherence to legal and ethical standards
- **Legal Review:** Regularly review whether the system's usage still meets legal and policy requirements
- **Reassessment Triggers:** Reassess the necessity and proportionality, if the system is repurposed or context changes
- **Monitoring Procedures:** Implement compliance monitoring mechanisms to track and document legal adherence (e.g., audits, alerts for boundary violations)
- **Updating Public Record:** Ensure procedures are in place for updates to the National Record of Processing Activities, if data practices change
- **Human Oversight:** Designate accountable personnel for legal oversight and establish a human-in-the-loop review process for high-impact decisions
- **Incident Reporting:** Establish clear reporting lines for legal, policy or ethics breaches; maintain logs of legal, policy or ethics breaches, with a clear process for escalation, reporting and corrective action
- **Remedy Procedure:** Establish responsibilities and mechanisms how to remedy legal and regulatory issues

AI Accountability responsibilities for migration/decommissioning

- **Transition Process:** When decommissioning or transitioning systems, verify legal compliance will be maintained (e.g., data protection, fair processing)
- **Continued Compliance:** Ensure the AI system is no longer processing personal data unless justified and logged
- **Preserve Documentation for Audit:** Archive legal assessments, data usage logs, compliance checks and decision records to support future reviews or legal inquiries in a format proven to facilitate long-term accessibility
- **Data Handling:** Securely delete, anonymise or archive data in line with data protection regulations
- **Full System Compliance:** Ensure third-party providers also comply with legal requirements during the migration/decommissioning processes, where applicable
- **Final Review:** Conduct a final review of the AI system's performance in line with legislative requirements, and any lessons learned for future procurements/deployments

Laws and Regulations considerations for intended users

Chief Officers

- **Legal Status:** What is the current law relating to AI?
- **Applicable Frameworks:** Which laws, regulations, guidelines, policies and frameworks apply to the AI system and AI use case?
- **Cross-Jurisdiction Use:** Will the AI system's outputs be provided to LEAs outside England, Wales, Scotland and Northern Ireland? If so, what other regulations and safeguards are to be followed?
- **Local Policy Validity:** What is the current organisational policy on using AI systems, and is it still in line with current law and regulations?
- **Policy Alignment:** Do organisational AI SOPs align with laws, regulations, guidance, policies and frameworks?

AI Users

- **Permission Compliance:** Are all the necessary permissions to use the AI system in place?
- **Codes of Practice:** Are the correct Codes of Practice being followed using the AI system?
- **Lawful Use:** Is the AI system being used in a legal, proportionate and justifiable way?
- **Ethical Use:** Are you confident your use of the AI system is consistent with ethical policing standards, particularly regarding fairness, transparency and legality?

Oversight Bodies

- **Legal Compliance:** Are you able to assess, given the information available, that the correct laws and regulations are being followed and enforced?
- **Risk Communication:** Have you communicated legal risks and areas for improvement to the policing organisation?
- **Regulatory Review:** Given the information available, are you able to review processes that pertain to adherence to relevant laws and regulations for the AI system (e.g., is there an up-to-date DPIA)?

Theme 4: Risk Assessment and Management

Purpose: This theme identifies risks, harms and biases associated with the AI system and implements mitigation measures. It covers both the impact of using and not using AI, with an emphasis on fairness and public safety. Identifying possible risk, harms and impacts of an AI system, as well as their likelihood is an important step to proactively manage these risks throughout the AI system lifecycle. It allows forward planning of how these risks (and associated harms) may be prevented, or where not possible, how they are to be managed, and robust mitigation measures to be put in place.

AI Accountability Principles addressed: Lawfulness, Proof, Completeness, Explainability, Transparency, Enforceability and Redress, Impartiality, Conduct, Learning

Guidance

Risks and harms assessment

Step 1: Assess the risks and potential harms associated with the AI system and its use

A comprehensive, proactive assessment of the potential risks associated with the AI system and its use helps the policing organisation to either prevent or prepare for their occurrence. The risk assessment can also establish whether deployment of an AI system poses a specific risk to particular communities and/or demographic groups.

A risk register should be created, listing the type of risks, who they may affect (and associated potential harms), as well as their likelihood and potential severity:

- **Risk Identification:** Identify risks associated with the AI system's procurement, deployment or migration/decommissioning (what could go wrong and to whom, e.g., individual, organisational, investigational integrity, community); also consider risks of not deploying the AI system
- **Harm Identification:** Determine uses or outcomes of the AI system that could potentially cause harm; consider type of harms and who these harms may affect
- **Likelihood:** Assess the likelihood of each identified risk; this assessment should be in line with methods used in wider organisational risk management
- **Severity:** Assess the probable severity if the risk was realised; compare against established risk criteria (e.g., legislative requirements, organisational thresholds) to determine levels of significance, whether they are acceptable and whether they require mitigation

The risk register should be reviewed on regular basis and after incidents.

Example - Risks to specific communities [xi]

The Royal United Services Institute (RUSI) report 'Data Analytics and Algorithmic Bias in Policing' (2019) reviewed the use of data analytics and algorithms in policing within England and Wales. Their findings highlighted over-reliance on automation risked imbedding discrimination within policing practice.

The research highlighted concerns that algorithms could inadvertently perpetuate or amplify existing bias against particular groups, particularly if training data reflects historical bias in police practice, replicating historic assumptions. However, issues can emerge across the system lifecycle, including data collection, model development, deployment and evaluation.

Step 2: Conduct key assessments to review risks

Conducting regular assessments about risks ensures that all foreseeable risks can be responsibly managed.

Such assessments should consider whether measures:

- Prevent or rectify data bias
- Address security, privacy and confidentiality requirements
- Identify and address unintended consequences of AI the system's data processing
- Manage information risks

S**everal key assessments can help supporting this aim:**

- Data protection compliance assessments
- Formal risk assessment
- Ethics assessment (including compliance with the Code of Ethics)
- Equality Impact Assessment
- Alignment with any established Codes of Practice

A policing organisation should conduct specific **cyber security risk assessments,** to ensure the integrity of the AI system and any infrastructure it utilises.

Step 3: Consider specific AI risks, misconduct and non-deployment

Particular AI risks: There are a number of potential risks which may be of concern in police use of AI. While they are not specific to the technology, they may be exacerbated in this context.

Bias and Discrimination	**Risk:**	AI systems trained on historical crime data can reflect and reinforce systemic biases, such as over-policing of certain communities.
	Example:	Predictive policing tools directing more proactive patrols to ethnic minority neighbourhoods, increasing arrests regardless of actual crime rates.
False Positives and Inaccurate Predictions	**Risk:**	Facial identification or predictive analytics can wrongly identify individuals as suspects, leading to detainment or surveillance.
	Example:	Misidentification of an individual could result in the arrest of an innocent party.
False Negatives and Inaccurate Predictions	**Risk:**	Facial identification or predictive analytics could fail to identify the offender as a suspect, leading to missed investigative opportunities.
	Example:	A failure to identify an individual as a potential suspect (where the system reasonably would have been expected to do so) may lead to missed investigative opportunities, unnecessary use of further resources and loss of public confidence in the system.
Lack of Transparency	**Risk:**	Decisions made by opaque AI models may not be explainable to those affected or operating the system, reducing AI accountability.
	Example:	A person may be denied bail from custody or labelled a flight risk without a clear reason that they or their legal representative can challenge.
Automation Bias	**Risk:**	Police officers or staff may over-rely on AI recommendations, treating them as infallible.
	Example:	A predictive tool flags someone as a weapons threat, and officers presume the individual is dangerous without questioning the output.
Function Creep	**Risk:**	AI tools introduced for narrow purposes (e.g., identifying stolen cars) may be expanded over time to broader, more invasive uses.
	Example:	A facial recognition system intended for serious crimes is later used to monitor the day-to-day movements of peaceful protestors.
Lack of Accountability	**Risk:**	When AI goes wrong, it is often unclear who is responsible – the developer, the policing organisation or the individual officers.
	Example:	Victims of algorithmic errors may struggle to seek redress due to complex responsibility chains.

Misuse: There are a number of potential risks posed by deliberate courses of action. Individual users may engage in misuse through unlawful access or processing of data. In this context similar risk management strategies should be implemented.

A further consideration would be the capability of a user to deny an AI system critical information as a data input. Here outcomes could be manipulated by skewing the information reviewed by the AI system. Issues of this kind are likely to be system and context specific but should be considered in the design process and usage policy.

Non-use: Where an AI capability is reasonably available for use, the implications of non-deployment must also be considered. This recognises that withholding AI in certain contexts may lead to negative outcomes or missed benefits. Considering the core policing duty of protecting life and limb, public safety requirements may dictate the use of the most effective lawful methods to achieve that aim.

Not engaging in AI use can thus represent a risk in and of itself, with missed opportunities to optimise policing activity, avert harm and provide a cost-effective service to the public. **Non-use should be an explicit part of the risk assessment and risk register.**

Risk and harm mitigation

Step 4: Define and regularly review mitigation measures

For each risk, mitigation measures should be included within the risk register. Practical mitigation procedures will be system specific, but may include:

- **Bias Auditing:** Testing of data and models for unfair outcomes or systemic bias
- **Adversarial Testing:** Using red team testing and simulation to assess continued resilience
- **Authentication and Authorisation:** Restrict who can access the system to those with a genuine purpose and appropriate training
- **Responsible Usage Policy:** Define and enforce appropriate use, including clear procedures to prevent uncritical acceptance of AI-generated outputs
- **Clear Responsibilities:** Every AI system in operation should have a clearly designated individual, accountable for the system's function, outputs and compliance with requirements of proper use
- **Monitoring and Logging:** Utilise routine logging, dip sampling, system behaviour and usage patterns, to detect abuse or anomalies
- **Human-in-the-loop:** Require human review for decisions impacting upon the public, i.e., a human must always serve as the ultimate decision-maker
- **Fail-safes and Shutdown Procedures:** Implement mechanisms to interrupt or stop the system if it behaves unexpectedly

Step 5: Consider specific mitigation issues of personal data

A particular matter of concern regarding the use of AI is its interaction with personal data. Deployers should be confident that:

- Any risk of bias in the processing of personal data has been mitigated
- Other risks relating to the AI system processing personal data are addressed

Special attention should be given to this topic with recorded assessments to detect and mitigate bias. Additional data protection and fairness risks should be reviewed continuously to ensure comprehensive safeguards are in place for all personal data processed by the system.

Residual risks: Where potential residual risks remain – despite legal compliance and procedures to address them – it should be evaluated whether such issues can be mitigated by procedure. Every reasonable effort should be made to eliminate all unlawful bias. However, no system is perfectly neutral, and it may be challenging to confirm total elimination in every use context. It is therefore important to include effective checks and safeguards within the method of deployment, in addition to data cleaning, to eliminate bias.

Risk Assessment and Mitigation considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Clear Ownership:** Individuals or teams responsible for overseeing AI procurement decisions are given formal responsibility for managing the risks involved in deploying the AI system and the associated risk mitigation strategies
- **Risk Forecasting:** AI system providers have communicated anticipated risks, including bias, privacy concerns and limitations of the system, and how they prevented, reduced or mitigated these risks in their system
- **Ethics and Impact Evaluation:** Ethical reviews, equality reviews, Equality Impact Assessments, etc. have been used to evaluate the suitability of the AI system for policing contexts generally, and the intended use case specifically
- **Transparency Requirements:** Contracts are in place that include obligations for explainability, audit access and the provision of documentation on model functionality and data usage
- **Beyond Value for Money:** Procurement decisions are based on demonstrable benefit to public safety and rights protection, not solely on cost-efficiency
- **Comparative Risk:** Consideration should be given to risks associated with the specific system being considered compared to other available systems or no system being procured at all

AI Accountability responsibilities during deployment

- **Operational Oversight Framework:** Governance structures effectively oversee ongoing use, including human-in-the-loop decision-making and continuous evaluation, to monitor known and emergence of new risks
- **Policy Implementation:** A Responsible Usage Policy is in place, including user training, limits on automation and mandatory human review
- **Bias and Impact Monitoring:** Methods are in place to monitor outputs for discriminatory patterns or systemic bias, particularly affecting vulnerable or historically disadvantaged communities
- **Incident Reporting Mechanism:** Robust mechanisms are established for users, and where applicable the public, to report concerns or harms resulting from AI use
- **Compliance Tracking:** The AI system effectively retains up-to-date logs of data use, decisions made and model performance for auditing and AI accountability purposes

AI Accountability responsibilities for migration/decommissioning

- **Residual Risk Review:** Lingering risks such as data retention, reputational damage or algorithmic bias in retained outputs have been identified and assessed
- **Data Management:** The archiving process anonymises or deletes sensitive personal data in accordance with legal and policy requirements
- **Lessons Learned:** Performance issues, stakeholder feedback and ethical challenges have been documented to inform risk management in future AI procurement and deployment
- **Accountability Continuity:** Risk assessment and management measures remain active through the decommissioning and post-use assessment phases
- **Transition Planning:** When replacing the AI system, risk mitigation, ethical review and user retraining are included in the transition plan

Risk Assessment and Mitigation considerations for intended users

Chief Officers

- **Strategic Accountability:** Have you ensured clear assignment of responsibilities, with a named individual accountable for risk assessment, monitoring and mitigation?
- **Governance Framework:** Are you confident that robust governance structures are in place that support the effective risk assessment and management?
- **Deployment Risk Assessment:** Have appropriate pre-deployment risk assessments been conducted (e.g., ethics, data protection, Equality Impact Assessment, etc.)?
- **Bias Mitigation:** Are reasonable measures in place to eliminate or mitigate bias across the AI lifecycle?
- **Policy Enforcement:** Are measures, such as the Responsible Usage Policy, and requirements for mandatory human oversight and decision-making, practically enforceable?
- **Operational Decision-Making:** Does your organisation have the tools to evaluate both the risks of using and not using AI?
- **Resource Allocation:** Are there sufficient resources for continuous risk monitoring, auditing and evaluation?
- **Community Impact Considerations:** Are ongoing measures in place to assure mitigation of disproportionate impacts on particular communities or demographic groups?

AI Users

- **Understand Limitations:** Do you avoid uncritical acceptance of AI outputs and decisions?
- **Human Oversight Role:** Do you recognise that users are responsible for final decisions and should not defer accountability to the AI system?
- **Bias Awareness:** Are you aware of potential biases in outputs and the steps needed to question and validate findings?

Oversight Bodies

- **Audit and Evaluation:** Have you incorporated the use of AI expressly within your internal and external audit arrangements?
- **Bias and Fairness:** Does your organisation have staff with sufficient technical understanding to scrutinise the AI system, identify bias and assess mitigation measures? (This may include assessment of data, algorithms and outcomes.)
- **Documentation and Transparency:** Do you have clear requirements for policing organisations on the documentation of usage policies, decision-making and AI accountability structures?
- **Ethical Compliance:** Do existing standards for ethical behaviour effectively encompassed police use of AI?
- **Misconduct and Misuse:** Do oversight and redress process have effective methods of monitoring and identifying signs of system misuse (e.g., unlawful access, intentional data skewing) and ability to assess whether safeguards are effective?
- **Non-deployment:** Do oversight processes account for whether a decision not to deploy AI in appropriate contexts represents a risk to public safety or service quality?
- **Risk Assessments:** Can you verify that formal risk assessments, ethics reviews and data protection compliance measures account for AI use?

Theme 5: Oversight and Redress

Purpose: This theme ensures mechanisms for independent scrutiny and AI accountability, allowing stakeholders, particularly the public, to challenge decisions and seek corrections, ensuring just outcomes.

- An appropriate **oversight process** ensures AI accountability through the effective monitoring and review of AI systems, their use, outcomes and impacts, and thereby compliance and integrity throughout the AI lifecycle.
- An appropriate **redress processes** support AI accountability in allowing stakeholders, including the public, a clear means to challenge decisions, correct mistakes and seek justice. Redress helps build trust, ensure fairness and demonstrates that a policing organisation's actions are subject to review and correction.

AI Accountability Principles addressed: Lawfulness, Proof, Explainability, Transparency, Compellability, Enforceability and Redress, Impartiality, Constructiveness, Conduct, Learning

Guidance

Oversight process

Step 1: Identify oversight requirements and process

Ensuring adequate oversight throughout the AI lifecycle is an integral part of AI accountability. Oversight refers to actions taken to review and monitor AI policies, plans and implementations, with the aim to ensure that (1) they achieve expected results, (2) represent value for money and (3) are compliant with relevant policies, laws, regulations and ethical standards.

A first step is to map out oversight requirements and related oversight procedures, i.e.,

- Legal requirements for oversight
- The areas and aspects that require oversight
- The procedures and mechanisms to implement and sustain adequate oversight
- The internal and external functions and organisations responsible for oversight (see Step 2)
- The information required to allow adequate oversight (see Step 3)

Step 2: Understand the type and nature of information being shared

A policing organisation needs to identify the oversight bodies that will be responsible for monitoring, assessing and enforcing the appropriate use of the AI system in their particular context, including potential conflicts of interests (see Theme 6 for considerations of stakeholder interests).

Oversight functions can be internal or external to the police organisation, as well as with a formal (legally mandated) or non-formal role.

Examples of internal groups:

- Functions ultimately responsible for the success of the AI efforts
- Individuals and policing functions using the AI capabilities

Examples of external groups:

- Legally mandated oversight bodies
- Groups most affected by the AI system and its deployment
- Communities concerned with the issue the AI deployment addresses
- Press and media organisations

For the implementation of an effective oversight process internal and external oversight functions need to work in alignment.

To accomplish this, a policing organisation should look to:

- Clarify the role and authority of the oversight bodies
- Understand the expected level of transparency and reporting
- Determine if there are any conflicts of interest

External bodies will vary depending on context. A non-exhaustive list of entities which may be involved in AI accountability oversight is provided in Appendix A 'Governance bodies with relevance for AI accountability'.

Step 3: Understand the type of information to be shared

The oversight process will require sharing of disparate types of information with each of the oversight bodies and groups.

A non-exhaustive list of information that may typically be requested for oversight purposes is:

- Purpose and scope of the AI system
- Data
- Model design and training
- Deployment context
- Decisions and outputs
- User behaviour
- Post-deployment monitoring
- Governance processes
- Risk register
- Impact assessments

In practicality, answering these questions will require creation and retention of materials such as:

Some information may be subject to a legal requirement to share, other information may be in the public interest to provide (e.g., for transparency purposes to retain public trust). Rationales, requirements and potential limitations to the sharing with each oversight body and group should be internally transparent. This transparency is also linked to Risk Management (discussed in Theme 4).

Sharing restrictions: Knowing what information a policing organisation can share will influence which and how information can be provided to different oversight bodies. If operational and security requirements restrict the ability to share information, police organisations still need to ensure that the AI system and its procurement, use, etc. will undergo scrutiny by appropriate independent assessors with appropriate clearance.

To help process this requirement a policing organisation should know:

- The operational or security requirements restricting the ability to share information to oversight bodies
- If it is in the public interest to share information, and if so, what information should be shared (e.g., algorithmic information, datasets, limitations of the AI system, outputs, deployment details)

Step 4: Identify how you are sharing the information

Once a policing organisation knows what information to share and who to share it with, communication mechanisms need to be established. These need to be targeted towards the respective audience (e.g., internal vs external oversight functions).

AI systems can be extremely complex and may require a data scientist or specialists to explain technical aspects. A policing organisation needs to ensure that the information is provided in a way the intended recipient will be able to understand; or there is a risk that the information is interpreted incorrectly and causes ill-informed or incorrect judgment on the AI system.

A policing organisation should further ensure that there is a clear method to feedback and record recommendations and requests made by an oversight body.

Redress process

Step 5: Establish a redress process

Redress ensures that there are consequences and/or remedies in case things go wrong. This includes appropriate corrections within the police organisation, AI system, its usage, etc., but can also extent to compensation or other forms of remedy. Adequate redress procedures provide fairness and integrity and are a corner stone of AI accountability.

An effective redress process includes:

- Information that affected individuals can understand, regardless of their technical or legal literacy
- Availability in multiple languages and formats, depending on audiences (e.g., online forms, via call centre staff, in-person support)
- Transparency regarding what decisions were made or influenced by an AI system
- Explanations of how the decision was reached and the role the AI system played
- Escalation procedures
- Procedures that operate promptly, with clear timelines for response and resolution
- Impartial review, ideally by decision-makers who are independent of the original decision
- Clear lines of responsibility for final outcomes, including implementation of corrections or compensation
- Maintainance of an auditable record of actions taken

Step 6: Monitor the redress process

The redress process will need to be reviewed and revised to ensure it remains fit-for-purpose, efficient, compliant and aligns with any change to legal or operational requirements. Lessons identified in the redress process should also be communicated to training and development teams, if applicable.

Erroneous outcomes produced by the AI system must be escalated to the developers/third-party for correction through a formal escalation process. This approach ensures the policing organisation maintains a central understanding on the scale and scope of any issues and can implement contingency measures if necessary.

It is important to focus on the purpose of accountability processes, to prevent a counterproductive and unresponsive form of compliance seeking. Regular and transparent evaluation ensures alignment with emerging risks and standards, ultimately fostering public trust in the process.

Oversight and Redress considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Oversight Role Identification:** Identify relevant oversight bodies and their role (ICO, ethics boards, HMICFRS, etc.)
- **Information Sharing Limits:** Determine operational/security limitations on information sharing
- **Information Definition:** Define what AI-related information can be shared (e.g., algorithms, datasets, protocols)
- **Redress by Design:** Include redress mechanisms in the AI system design
- **Lead Assignment:** Assign responsibility for oversight and redress to internal leads

AI Accountability responsibilities during deployment

- **Engagement Channels:** Establish targeted engagement channels with oversight bodies and core stakeholders
- **Public Transparency:** Where possible, update public-facing information to help build trust
- **Redress Monitoring:** Establish and monitor the redress process and adjust where necessary

AI Accountability responsibilities for migration/decommissioning

- **Oversight Notification:** Notify all relevant oversight bodies before migration or decommissioning
- **Redress Resolution:** Resolve outstanding redress issues
- **Data Assurance:** Confirm all data has been securely removed or migrated
- **Final Review:** Conduct final oversight review of the AI system's performance
- **Documentation Archiving:** Archive any relevant documentation such as decision logs and redress records
- **Asset Register Update:** Update the Information Asset Register accordingly

Oversight and Redress considerations for intended users

Chief Officers

- **Oversight Identification:** Have the correct and relevant oversight bodies been identified for this AI system and use purpose?
- **Redress Mechanism:** Is there an accessible and appropriate redress process in place that specifically accounts for harms or disputes arising from the AI system?
- **AI Accountability Leads:** Are there designated responsible leads within the organisation for managing oversight and redress processes?
- **Feedback Integration:** Are findings, recommendations or requirements (such as lessons learnt or directives) from oversight bodies systematically fed back into operational practice and policy?

AI Users

- **Information Restrictions:** Are operational and security-based restrictions on information sharing clearly documented, and do you understand how they apply to your role?
- **Error Identification:** Can you identify and report anomalies, biases or errors in the AI system – including those caused by user behaviour or input?
- **Reporting Compliance:** Are you following reporting procedures (internal and external) when an issue or concern related to AI deployment arises?
- **Operational Feedback:** Are you actively providing operational feedback to support oversight reviews and improve system performance?
- **Disclosure Protocol:** Are you complying with organisational policy on information disclosure, especially with regard to oversight bodies and sensitive or classified information?

Oversight Bodies

- **System Review:** Is the review of the AI system's use and outputs fully independent and unfettered?
- **Compliance Monitoring:** Does the policing organisation demonstrate compliance with relevant laws, regulations and policies?
- **Transparent Communication:** Does communication of findings regarding the AI system fit into existing feedback structures?
- **Oversight Integrity:** Is the independence, expertise and impartiality of oversight activities assured by sufficient ability to interpret the technical aspects of AI use?
- **Redress Effectiveness:** Are redress mechanisms in place and evaluated to ensure their continued relevance and effectiveness?

Theme 6: Identification and Management of Stakeholders

Purpose: This theme aims at mapping and engaging all relevant parties who are involved in or affected by the AI system. This includes those internal to the policing organisation, external parties such as AI developers or oversight bodies and members of the public. A thorough identification and management of stakeholders ensures that:

- A full picture of which relevant groups, bodies and organisations are responsible for AI accountabilities (e.g., oversight bodies, affected communities, AI providers) and their respective roles is available
- A proactive management strategy for how to communicate and engage with these stakeholders in effective ways is in place along with a clear strategy for how to respond to challenges, information requests or audit

AI Accountability Principles addressed: Lawfulness, Completeness, Inclusivity, Explainability, Transparency, Compellability, Enforceability and Redress, Impartiality, Constructiveness, Conduct

Guidance

Identification of AI Accountability stakeholders

Step 1: Identify all stakeholders relevant for this AI lifecycle phase

Relevant stakeholders are those that either:

- Use the AI capability or outputs of the AI capability for policing purposes
- Have responsibility to make design, procurement, deployment and/or decomissioning decisions
- Are performing oversight functions
- Are affected by the AI capabilities
- Need to be informed about the AI procurement, deployment, etc. for other reasons

For a comprehensive identification consider the 4 categories (see Appendix A for a non-exhaustive list of examples):

Police-internal functions	Governance bodies	Specific communities and general public	External organisations and expert groups

Guiding questions that a policing organisation should consider include:

- What criteria are used to identify relevant stakeholders?
- Do any of the stakeholders have protected characteristics that need special treatment/consideration?

Step 2: Ensure that stakeholders are reviewed at important points of the AI lifecycle and if needed updated

Different stakeholders will become relevant at different points of an AI lifecycle. A policing organisation can optimise efficiency by ensuring that they are engaging with the correct stakeholders and to the correct extent.

To achieve this, a policing organisation should consider:

- Which points of the AI lifecycle are relevant to which stakeholders?
- What communication is required and to what extent?
- What risks arise if the stakeholder is not properly engaged with?

Management of stakeholders

Step 3: Define the communication and engagement requirements for each stakeholder, how this will be done and who is responsible for the communication/engagement

A policing organisation needs to consider their audience when communicating to stakeholders and ensure that the communication is received as intended. Active stakeholder management enables clear communication, coordinated decision-making, and early identification of concerns. Although a policing organisation will decide what it communicates and when, transparency is encouraged during all engagement to help build trust, clarity and understanding.

Communication and engagement requirements can be:

- To inform or require information from a stakeholder
- To provide or request evidence, materials or documentation
- To support financial or legal accountability

Guiding questions to consider are:

- Are there access restrictions across stakeholder groups for the sharing of information, decisions, data, etc?
- Can they be explained/evidenced?

Step 4: Account for stakeholder groups that will require additional considerations to communicate or engage with and how to ensure that they still receive adequate information

Diverse populations will receive and understand information differently; therefore, it is crucial that the policing organisation takes measures to reduce potential barriers or challenges.

Example challenges can be:

- Low trust towards police
- Special requirements for communication or access to information, including language or impairments/disabilities and available technology

Step 5: Define how successful communication and engagement will be assessed and put counter-measures in place, in case they fall short

To establish meaningful stakeholder communication and engagement, it is helpful to create criteria that communications and engagement efforts can be evaluated against. This will help to ensure that messages are clear, impactful and appropriate for the intended audience.

A policing organisation should consider whether:

- Communication has successfully increased awareness
- The communication cycle includes information on how concerns have been addressed appropriately
- The communication strategy addressed negative impacts and information about complaints/redress procedures

The measurement of effect needs to be quantifiable and link the exposure (of the message) to an outcome (e.g., sentiment towards the police and the AI system). Typically, this can be achieved through community engagement.

Step 6: Outline potential concerns and expectations of general public/society that may cause challenges to the AI deployment and how to address them

Public concerns such as privacy invasion, bias and intrusive surveillance can significantly influence the acceptance or rejection of an AI system. By identifying these challenges early, developers and policymakers can take proactive measures to address them through design, transparency and engagement.

A policing organisation should seek to:

- Identify all possible concerns that the public may have with the police use of the AI system
- Address concerns before they become an issue (control the narrative)
- Have contingency communication plans in place, particularly if the engagement reveals a high level of opposition

Stakeholder considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Stakeholder Identification:** Identify relevant stakeholders and include them in the procurement process (e.g., oversight bodies, police procurement officers, legal advisors, external topic experts)
- **Communications Planning:** Create a communication plan in order to engage with relevant stakeholders, including the public about the intended AI system use
- **Guidelines:** Articulate the intended aims and scope of the AI system use into a formal project proposal
- **Due Diligence:** Ensure that all parties involved in the development and provision of the AI system have been identified and appropriately assessed
- **Stakeholder Involvement:** Ensure that legal, technical, ethics and community oversight stakeholders have been engaged early in procurement deliberations

AI Accountability responsibilities during deployment

- **Stakeholder Communication Protocol:** Identify if any stakeholders should be informed of deployments, on what timescales and by what means
- **Operational Insight and Data Sharing Requirements:** Establish if any stakeholders require insight into decisions or access to ongoing operational data
- **Final Deployment Responsibility:** Identify who is accountable for final deployment decisions, including pausing or stopping deployments
- **Data Retention and Documentation:** Identify what information, data or materials need to be recorded or retained, under what authority and in what format, to ensure long-term AI accountability towards relevant stakeholder groups
- **Public Trust:** Address identified public concerns about police use of AI through transparency and communications strategy
- **Transparency and Disclosure:** Ensure a process for affected stakeholders to be informed, if an adverse incident takes place
- **Feedback and Complaint:** Ensure affected stakeholders can inform police about (potential or actual) negative impacts

AI Accountability responsibilities for migration/decommissioning

- **Stakeholder Continuity:** Identify stakeholders relevant to decommissioning decisions, including the impact of withdrawal or replacement of the AI sytem
- **Communications Planning:** Identify who needs to be informed about migrations and decommissioning, including their implications and impact
- **Ongoing Accessibility:** Identify who will have, or needs, access to data, information and materials from decommissioned systems and likely time scales
- **Data Protection:** Maintain processes to facilitate deletion of data as required by data protection legislation, policy or in response to requests from affected stakeholders
- **Public and Internal Communication:** Clearly communicate the system's decommissioning to stakeholders and affected individuals, especially where trust, rights or services are involved

Stakeholder considerations for intended users

Chief Officers

- **Stakeholder Mapping:** Are you confident that a comprehensive and up-to-date mapping of all relevant stakeholders across the AI lifecycle has taken place?
- **Internal Collaboration:** Have you mandated cross-departmental reviews to capture diverse internal and external perspectives in stakeholder identification?
- **Responsibility Assignment:** Have clear responsibilities been assigned within the Chief Officer team, and to relevant leaders in the organisation, for managing stakeholder communication and engagement?
- **Inclusive Engagement:** Are strategies in place to effectively engage communities with protected characteristics or low trust in police?
- **Public Expectations:** Have you identified potential concerns and expectations from the public and accounted for this in both AI deployment and corporate communication?
- **Evaluation Measures:** Are there measures for assessing communication and engagement success, and are there procedures for corrective action, when standards are not met?

AI Users

- **Stakeholder Awareness:** Are you aware of who the relevant stakeholders are, and how your use of the AI system impacts them?
- **Access Restrictions:** Do you understand and follow the access restrictions related to information sharing across different stakeholder groups?
- **Information Flow:** Are you clear on your role in passing information to oversight bodies or responding to public or governance queries?
- **Community Interaction:** Are you prepared to engage appropriately with affected communities, recording, reporting and actioning any concerns they express about AI use?
- **Process Updates:** Are you involved in or informed of updates to stakeholder management processes that could affect your operational use of the AI system?

Oversight Bodies

- **Stakeholder Identification Review:** Have you verified that the police have conducted an inclusive and systematic identification of all relevant stakeholders?
- **Lifecycle Triggers:** Are mechanisms in place to ensure stakeholder reviews are triggered at key lifecycle stages (e.g., moving from piloting to deployment)?
- **Transparency Check:** Have you assessed whether communication and engagement strategies are transparent and fair across all stakeholder groups?
- **Equality and Diversity:** Have you evaluated how the policing organisation ensures effective engagement with all of the communities it serves?
- **Documentation Audit:** Is there clear, accessible documentation showing how stakeholder voices have been integrated into decision-making and governance?
- **Public Concern Oversight:** Are you monitoring how the police identify and respond to societal and public concerns regarding AI deployment?
- **Public Engagement:** Is appropriate community input and transparency used to build trust in AI use in policing and prevent alienation or suspicion?

Theme 7: Accountability Evidence

Purpose: This theme ensures that evidence, about how AI accountability is assessed and captured, is robust, verifiable, accessible and understandable. This is not about criminal evidence but how policing evidences its AI accountability. By knowing how to prove AI accountability correctly, a police organisation will be better positioned to respond to challenges. The process will also highlight areas of AI accountability, which may need developing further.

AI Accountability Principles addressed: Lawfulness, Proof, Completeness, Inclusivity, Explainability, Transparency, Compellability, Enforceability and Redress, Constructiveness, Conduct, Learning

Guidance

Creation of robust evidence

Step 1: Define the criteria for robust and sufficient evidence

Although there might be criteria that are specific to each policing organisation, or even each AI system and its intended use, **the criteria that can guide what should be considered as AI accountability evidence should align with:**

- Requirements by law
- Additional regulatory requirements
- The Code of Ethics requirements
- National (NPCC) Strategy, Policy and Guidance
- Regional/Local Policy and procedure
- Criminal evidence integrity
- Requirements of stakeholders and oversight bodies

A policing organisation will need to decide which information best demonstrates AI accountability to capture and document the relevant and appropriate evidence ('proof') across all themes.

This evidence of AI accountability, or proof, will be important in numerous contexts. For example, it can be used to support operational cases through criminal justice processes demonstrating, and where required, the legality and integrity of the AI system in question. Proof will also assist in maintaining public confidence and consent, through the transparent demonstration of AI systems being used, their function and their utility.

Example - Failing to acquire proof [xii]

In Bridges v South Wales Police, the Court of Appeal ruled that South Wales Police failed to comply with the Public Sector Equality Duty when deploying facial recognition technology as they did not take reasonable steps to investigate whether the system could produce biased outcomes based on race or sex. Although there was no clear evidence that the system was biased, the failure to assess for possible biases was itself a breach of duty.

Step 2: Build processes to collect AI accountability evidence

To ensure AI accountability evidence is being recorded, a policing organisation should seek to embed AI accountability collection methods into the AI systems lifecycle, including the AI system itself. Standardised procedures that are consistent across departments should be developed and should be co-created with support from governance, legal and technical teams to ensure the right data is being recorded and to maximise usability.

When creating a process to record AI accountability, a policing organisation should consider including data such as:

- **What** AI accountability evidence needs to be recorded?
- **When** does it need to be recoded, and for how long?
- **Where** is the data going (has it been sanitised; can it be disclosed)?
- **Why** is the data recorded (does it add value to service accountability)?
- **How** is the data recorded (is it accessible, usable, secure and archived correctly)?

At each stage of the AI system's lifecycle, it is recommended that AI accountability proof is reviewed to ensure completeness.

Safeguarding evidence

Step 3: Enable correct accessibility

A policing organisation must ensure that the evidence used to demonstrate AI accountability for their AI system complies with any legal or policy requirements that govern information/material handling and disclosure. However, a balance needs to be struck in that the proof of accountability must also be accessible to all relevant stakeholders and oversight bodies in order to support transparency and effective oversight. The information communicated needs to be in a clear and understandable format, ensuring that both technical and non-technical audiences can use the information appropriately (see Theme 6).

To ensure evidence of AI accountability is both useful and accessible, a police organisation should follow the MTbD principle in how that information is communicated and shared. This means tailoring information such as algorithmic documentation, deployment records or risk assessments to the needs and technical understanding of various oversight bodies and stakeholders.

A controlled access framework should be established so that the right stakeholders can view the necessary information without compromising operational sensitivity or data protection obligations.

AI Accountability Evidence considerations throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Procurement Decision Records:** All decisions related to the procurement of the AI system must be formally recorded; this should incorporate necessity considerations
- **Third-Party Disclosure Requirements:** Developers or third-party providers must meet disclosure requirements, including providing technical information such as training data
- **Demonstrating Accountability Evidence:** The policing organisation must be able to demonstrate to stakeholders and oversight bodies that it is collecting and maintaining the correct AI accountability evidence
- **Procurement Disclosure Safeguards:** Control measures must be established to protect against unnecessary or unlawful disclosure of procurement-related information

AI Accountability responsibilities during deployment

- **Deployment Evidence Recording:** The organisation must record appropriate AI accountability evidence throughout the deployment of the AI system
- **Ongoing Transparency:** Standards of transparency must be maintained to demonstrate proper evidence collection to stakeholders and oversight bodies
- **User Interaction Monitoring:** User interactions with the AI system must be monitored and auditable to ensure responsible use and system traceability
- **System Update Logging:** All updates to the AI system must be logged and justified
- **Operational Disclosure Safeguards:** Measures must be in place to prevent unnecessary or unlawful disclosure during system operation
- **Records of Performance Evidence:** Evidence related to system performance, audit trails and decision logs must be retained in line with local policy and legislative requirements

AI Accountability responsibilities for migration/decommissioning

- **Migration and Decommissioning Records:** The organisation must record and review all steps involved in the secure migration or decommissioning of the AI system
- **Archiving Performance Evidence:** Evidence related to system performance, audit trails and decision logs must be archived appropriately
- **Accessibility of Archived Data:** Archived data must be accessible in case decisions need to be revisited
- **Documentation of Decisions:** All decisions made during migration/decommissioning must be documented and justified
- **Disclosure Safeguards:** Safeguards must remain in place to prevent unlawful or unnecessary disclosure or retention during and after migration/decomissioning

AI Accountability Evidence considerations for intended users

Chief Officers

- **Assigned Responsibilities:** Have clear responsibilities been assigned for recording and maintaining accountability evidence at all stages of the AI system's lifecycle?
- **Oversight for External Scrutiny:** Is there oversight in place to ensure decisions made under your authority can be explained and justified?
- **Periodic Review Mechanisms:** Have mechanisms been put in place to periodically review AI accountability evidence?

AI Users

- **Awareness of Evidence Requirements:** Are you aware of what types of AI accountability evidence you are expected to (and not to) record?
- **Access to Systems:** Do you know how to access the tools and systems required to document your use of the AI system?
- **Reporting Procedures:** Are procedures in place for you to record unexpected behaviours, impacts or performance issues in the AI system or user error?
- **Data Migration and Decommissioning:** Have the steps for secure data migration or decommissioning been recorded and reviewed?
- **Disclosure Controls:** Are there control measures in place to protect against unnecessary or unlawful disclosure?

Oversight Bodies

- **Access to Records:** Do you have access to comprehensive, understandable records showing how and why the AI system is procured/used/decommissioned?
- **Documentation Provided:** Has the policing organisation provided you with sufficient technical and operational documentation to enable meaningful scrutiny?
- **Information Format Suitability:** Is the format in which information is shared suited to your review and reporting requirements?
- **Evidential Integrity:** Are you able to verify the integrity of AI accountability evidence, and trace how decisions about it were made and recorded?
- **Alignment with Standards:** Can you assess whether the AI system's use aligns with legal, ethical and policy standards, and whether gaps in AI accountability have been identified and addressed?

Theme 8: Adaptability and Learning

Purpose: Adaptability and Learning ensures that policing stays up-to-date with technological innovations or requirements in AI and societal changes. It encourages continuous improvement through feedback, review and learning. It thus ensures that:

- Procedures and skills are reviewed and updated where necessary
- Those developing or using the AI system remain aware of their responsibilities
- Lessons are learned from mistakes, inefficiencies or unexpected/negative consequences

AI Accountability Principles addressed: Lawfulness, Inclusivity, Transparency, Compellability, Enforceability and Redress, Conduct, Learning

Guidance

Continuous improvement

Step 1: Embed learning and adaptability early

As governance requirements, AI technologies and social attitudes change, a policing organisation will need to keep current with their demands and needs. For an AI system to remain current and safe, continuous improvement needs to be designed into all parts of the AI lifecycle and ecosystem. Early adoption of the requirement for learning and adaptability will help a policing organisation become dynamic and responsive to changes outside of their control. **Adaptability and Learning thus needs to be designed in throughout the AI lifecycle.** Contractual agreements to third parties for example, should explicitly make previsions for the need of an AI system to be responsive and unplanned updates may be required.

Consideration should be given to:

- Where along the AI lifecycle adaptability will be required
- Development of a road map for lessons to be identified across the AI lifecycle to support learning (individual or organisational), e.g.. on:
  - Procurement contracts
  - Tradecraft
  - The AI system
  - Processes
  - Management and governance

Step 2: Up-skill the organisation

A general AI awareness will be required of staff. This is similar to generalised data protection or fire safety knowledge requirements expected of the full workforce and should provide awareness of general principles of responsibility for using AI accountably. This prepares policing for a future where AI use is deeply imbedded into routine organisational functions and operational policing. It also ensures policing has an understanding of how external parties using AI may impact upon them. This awareness should include knowledge of monitoring processes and contextualised understanding of the consequences for breaches.

To achieve this, a policing organisation should consider:

- Training for users (including managers)
- Raising awareness for those not directly involved

Step 3: Continually review, feedback and adapt

Processes should be put in place, where a policing organisation can record lessons learnt that can then be fed back into the AI ecosystem. The process will need to include lessons identified during all stages of the AI lifecycle.

To support this process, the organisation should:

- Ensure there is a learning feedback loop at all stages of the AI lifecycle
- Assign responsibility to manage and implement changes (e.g., does this information need to be provided to training and development teams or to AI developers?)
- Monitor and adjust to new changes to ensure they are effective and correct

Adaptability and Learning throughout the AI lifecycle

AI Accountability responsibilities for procurement

- **Training Information:** Confirm providers/developers provide sufficient system information for an effective training course on the system
- **Future Proofing:** Embed requirements for ongoing system adaptability as a core procurement requirement
- **Ongoing Improvements:** Guarantee long-term developer involvement and lifecycle support
- **Adaptability:** Include adaptability metrics in system evaluation, such as capacity for retraining, patching, as well as integration of feedback

AI Accountability responsibilities during deployment

- **Training Assurance:** Implement structured training, communicating requirements and expectations appropriate to the user's role
- **Base Level Knowledge:** Maintain a core level of organisational AI knowledge delivery provision to all staff, as well as specific training for AI system users
- **Integration of Feedback:** Confirm feedback channels for reporting issues, errors or suggested updates to result in meaningful improvement
- **Proactive Monitoring:** Ensure monitoring processes proactively identify areas in which the system is functioning sub-optimally, allowing adaptation and mitigation
- **Collaborative Improvement:** Maintain continuous collaboration between developers, deployers and end users to integrate updates and learning
- **Continual Development:** Avoid treating deployment as a static endpoint, and build in mechanisms for ongoing improvement and responsiveness to emerging risks

AI Accountability responsibilities for migration/decommissioning

- **Organisational Memory:** Ensure any new or replacement AI system benefits from cumulative learning, rather than a functionality reset with each new AI system
- **Reflective Practice:** Use migration or decomissioning as an opportunity to reflect on the effectiveness of feedback and improvement mechanisms, to benefit future systems
- **Full Lifecycle Evaluation:** Evaluate how the system adapted (or failed to adapt) over time, as part of knowledge transfer and organisational learning
- **Comprehensive Review:** Included all involved parties, including developers, users and other stakeholders in the review process

Adaptability and Learning considerations for intended users

Chief Officers

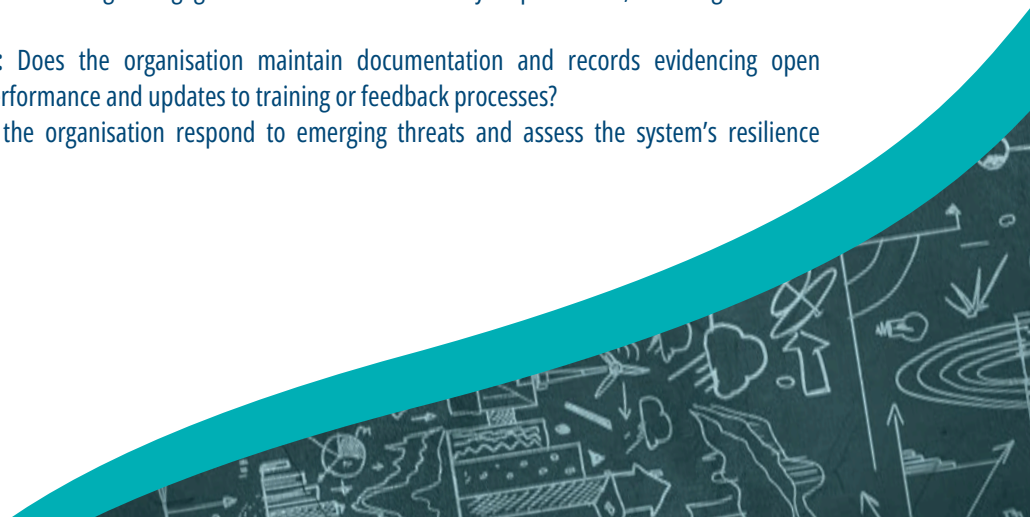
- **Building Base Level Knowledge:** Is AI awareness built into routine organisation-wide training (akin to data protection or fire safety)? Do the users of AI systems within the organisation have sufficient knowledge to fulfil their roles and accountability requirements appropriately and comprehensively?
- **Setting Expectations:** Have you effectively and consistently communicated that adaptability and continuous learning are part of expected AI use within your organisation?
- **Support Feedback Structures:** Are you confident there are robust mechanisms for user feedback and that issues raised are taken seriously and escalated where needed?
- **Sustain Developer Engagement:** Are agreements in place for your enabling services teams to have long-term collaboration with developers, to maintain and improve the system post-deployment?
- **Anticipate Change:** Does your review process ensure adaptability in reaction to external developments (e.g., emerging vulnerabilities of the AI system, regulatory shifts, etc.) in both risk management and operational strategies?
- **Proactive Change:** Do regular system reviews proactively identify methods of improved practice, both technical and procedural?

AI Users

- **General Awareness:** Have you developed a baseline understanding of AI and sufficient knowledge of the AI systems you will directly use, including ethical, legal and AI accountability considerations?
- **Ongoing Training:** Have you participated in required training, including refresher training, to understand evolving system capabilities and expectations?
- **Feedback Responsibility:** Do you know how to report issues, errors or misuse through clearly defined channels, whether system-integrated or organisational?
- **AI Accountability in Practice:** Do you understand the specific consequences of misuse or process breaches for the AI system you use?
- **Adaptive Use:** As the AI system evolves, are you able to adjust practices to maintain effectiveness and integrity?
- **Understand Monitoring:** Are you aware of how system use is monitored and how this relates to performance and compliance evaluations?
- **Documented Processes:** Do you know how to access process documentation?

Oversight Bodies

- **Training Content:** Does the syllabus and its ethos meet required standards of quality assurance?
- **Equality:** Are considerations relating to diversity and equality in AI use effectively covered by training?
- **Continuous Review:** Do organisational accountability processes exist to ensure the police organisation remains responsive to technological and legislative developments?
- **Evaluate Feedback Process:** Are feedback mechanisms effective and accessible, resulting in demonstrable improvements?
- **Culture of Compliance:** Is there meaningful engagement with AI accountability requirements, fostering trust and transparency?
- **Improvement Transparency:** Does the organisation maintain documentation and records evidencing open communication about system performance and updates to training or feedback processes?
- **Threat Benchmarking:** Does the organisation respond to emerging threats and assess the system's resilience against them?



Appendix A: Core Accountability Stakeholders

Please note: The overview is not intended to be exhaustive and will differ depending on the context of use and UK Legal Jurisdiction(s) the system is used within.

Police-internal AI Accountability stakeholders

- Chief Constable/Chief Officers
- Enabling Services, such as
  - Procurement Professionals
  - IT Department
  - Information Management
  - Data Assurance/Protection
  - (AI) Product Sponsor
  - Corporate Communications
  - Legal Services
  - Training Professionals
- Users deploying the AI system
- Functions that make decisions based on AI outputs
- Functions that provide data for AI training or AI deployment
- Staff otherwise impacted by the AI system

Governance bodies with relevance for AI Accountability[xiii]

England and Wales:

- His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMRCFRS)
- Independent Officer for Police Conduct (IOPC)
- HM Courts and Tribunal Service
- Local Elected Policing Bodies

Northern Ireland:

- NIPB
- His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMRCFRS)
- Criminal Justice Inspection Northern Ireland
- Police Ombudsman's Office
- HM Courts and Tribunal Service
- Chief Human Rights Commissioner
- Local Elected Policing Bodies

Scotland:

- SPA
- His Majesty's Inspectorate of Constabulary in Scotland
- Police Investigations and Review Commissioner
- Scottish Information Commissioner
- Local Elected Policing Bodies

Cross-Jurisdictional:

- Information Commissioner (England and Wales, Northern Ireland, limited involvement in Scotland)
- Investigatory Powers Commissioner (IPC)
- Equality and Human Right Commission

External organisations and bodies

- Industry/developers from which AI capabilities are procured
- Interest groups, such as:
  - Business groups, Chambers of Commerce, Trade Unions
  - Private security
  - Transport providers
  - Equalities groups
- Press and media

Public and special communities

- Communities with special interests, such as
  - Children and youth
  - Groups with disabilities
  - Rural communities
  - Religious communities
  - Environmental groups
- Specifically impacted or affected communities, including minorities and vulnerable groups
- Groups with Protected Characteristics (Equality Act 2010)

Appendix B: Lifecycle Legislative Considerations

The below table is an illustration of laws, regulations, guidance and frameworks a policing organisation may need to consider at each stage of an AI system's lifecycle. This table is not exhaustive and may change as new laws and regulations come into force.

Name	Development/ Procurement	Deployment	Migration/ Decommission
UK GDPR 2018	✓	✓	✓
Data Protection Act 2018	✓	✓	✓
Human Rights Act 1998	✓	✓	✓
Equality Act 2010	✓	✓	✓
FOI Act 2000	✓	✓	✓
National Artificial Intelligence Cyber Standard	✓	✓	
National AI Strategy	✓		
Using artificial intelligence in the public sector	✓	✓	
Guidelines for AI procurement	✓		
GovS Functional Standards	✓		
ISO (e.g., 42001, 17020, 17025)	✓	✓	✓
Cyber Essentials	✓	✓	
ICO AI and data protection	✓		
ICO Explaining decisions made with AI	✓	✓	
ICO Biometric data Guidance	✓	✓	
Police and Criminal Evidence Act 1984		✓	
Regulation of Investigatory Powers Act 2000		✓	
Investigatory Powers Act 2016		✓	
AI Accountability in Policing and Security	✓	✓	✓
College of Policing Code of Ethics	✓	✓	✓
Codes of Practice	✓	✓	✓
Covenant for Using Artificial Intelligence (AI) in Policing	✓		
NPCC ALGO-CARE	✓	✓	
Force Policy	✓	✓	✓
Policy Decisions		✓	

Appendix C: Glossary

Advanced Data Analytics
The use of complex techniques and tools, such as machine learning, predictive modelling or statistical analysis, to extract insights, identify patterns, or support decision-making from large or complex datasets.

AI (Artificial Intelligence)
The capability of a machine to perform tasks that typically require human intelligence, such as learning, reasoning or decision-making.

AI System
A system that uses AI technologies, such as machine learning, to perform tasks, make decisions or generate outputs, often with a degree of autonomy.

AI Ecosystem
The interconnected network of all entities (e.g., people, data, processes, legal and regulatory frameworks) that are influenced by, or influence the AI lifecycle, including outputs.

AI User
An individual or department that deploys, operates or relies on the outputs of an AI system. This includes those involved in initial procurement, local oversight, implementation or direct use of the system in decision-making.

Algorithm
A set of rules or instructions given to an AI system to help it learn, solve problems or perform tasks.

Bias (in AI)
A systematic error in an AI system that can lead to unfair outcomes, often due to flawed data or assumptions.

Machine Learning (ML)
A subset of AI where systems learn from data and improve their performance over time without being explicitly programmed.

Bibliography

[i] Akhgar, B., Bayerl, P.S., Mounier, G., Linden, R. and Waites, B. (2022). AP4AI: Accountability Principles for Artificial Intelligence in the Internal Security Domain. European Law Enforcement Research Bulletin, Special Conference Edition, 6. Available at: https://shura.shu.ac.uk/31123/ [Accessed 13 March 2025].

[ii] National Police Chiefs' Council (NPCC). (2023). Covenant for Using Artificial Intelligence (AI) in Policing. [online] Available at: https://science.police.uk/site/assets/files/4682/ai_principles_1_1_1.pdf [Accessed 18 April 2025].

[iii] Office for Artificial Intelligence (2020). Guidelines for AI procurement. [online] HM Government. Available at: https://www.gov.uk/government/publications/guidelines-for-ai-procurement/guidelines-for-ai-procurement [Accessed 30 April 2025].

[iv] College of Policing (2024) Code of Ethics. Available at: https://www.college.police.uk/ethics/code-of-ethics [Accessed: 11 May 2025].

[v] Novelli, C., Taddeo, M. and Floridi, L., (2023). Accountability in artificial intelligence: what it is and how it works. AI & Society, 39, pp.1–12. https://doi.org/10.1007/s00146-023-01635-y.

[vi] Akhgar, B. & Bayerl, P.S. (2024). 'How to do AI accountability – and why it's worth the effort', in Higgins, A. & Halkon, R. (eds.) Policing and the Fourth Industrial Revolution: Cumberland Lodge Police Conference 2024 – Conference Report. London: The Police Foundation, pp. 16–17. Available at: https://www.police-foundation.org.uk/wp-content/uploads/2010/10/cumberland-lodge-2024.pdf [Accessed: 6 May 2025].

[vii] Akhgar, B., Bayerl, P.S., Mounier, G., Linden, R. and Waites, B. (2022). AP4AI: Accountability Principles for Artificial Intelligence in the Internal Security Domain. European Law Enforcement Research Bulletin, Special Conference Edition, 6. Available at: https://shura.shu.ac.uk/31123/ [Accessed 13 March 2025].

[viii] Office of the Police Chief Scientific Adviser (OPCSA). (2024). UK Police Industry Charter. [Online] Available at: https://science.police.uk/site/assets/files/5011/police_industry_charter.pdf [Accessed 11 May 2025].

[ix] Information Commissioner's Office (ICO). (2023). What about fairness, bias and discrimination? Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/ [Accessed: 28 April 2025].

[x] Information Commissioner's Office (ICO). (n.d.). Metropolitan Police gangs matrix. Available at: https://ico.org.uk/for-the-public/ico-40/metropolitan-police-gangs-matrix/ [Retrieved 29 April 2025].

[xi] Babuta, A. and Oswald, M. (2019). Data Analytics and Algorithmic Bias in Policing. London: Royal United Services Institute. Available at: https://assets.publishing.service.gov.uk/media/5d7f6b2540f0b61ccdfa4b80/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf [Accessed 1 May 2025].

[xii] Judiciary of England and Wales. (2020). R (Bridges) v Chief Constable of South Wales Police and others: Press Summary. [online] Judiciary UK. Available at "https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Press-Summary.pdf"https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Press-Summary.pdf [Accessed 30 April 2025].

[xiii] House of Lords Library. (2020) Policing in the UK: Governance, Oversight and Complaints. [Online]. London: House of Lords Library. [Accessed 26 March 2025]. Available from: https://lordslibrary.parliament.uk/research-briefings/lln-2020-0013/.

Methodology

The development of the guidance followed a process of scoping and objectives definition, particularly through Delphi studies with practitioner experts. These expert consultations identified key user groups, stakeholders and the specific challenges related to AI accountability in policing. This work was additionally informed by horizon scanning of the legal and regulatory landscape, including NPCC, OSCE, ISO related standards, BSI (42001). Architectural reconstruction was employed to identify intended users, with the aim of the development of user-focused, actionable content.

Structure development was then guided by the identified chronological stages of a policing procurement processes which was overlayed with AI accountability requirements across the AI system lifecycle. These were placed within a 'Theme' structure based on groupings of identified AI risks. The theme structure draws on existing understandings of risk grouping and insights from the expert consultations. To operationalise the guidance, concepts of AI accountability were distilled into a series of practical, question-based prompts designed to support decision-making at each stage of system adoption and oversight.

A second process of stakeholder engagements took place, consulting with experts in data protection and public procurement, as well as further policing practitioners.

The guidance document was thus developed through an iterative and phased process to ensure relevance, clarity and practical application. The guidance, by design, is AI system agnostic allowing for adaptability in use across all deployments. This approach enhances usability and futureproofing by ensuring the guidance remains relevant as AI capabilities evolve and new tools emerge.

The AIPAS project

The AIPAS project is a UK-based initiative focused on developing practical tools and frameworks to help policing organisations implement AI accountably and aligned with public expectations.

AIPAS is led by **CENTRIC** (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research) and delivered in collaboration with:

- Innovate UK
- North East Business Resilience Centre (NEBRC)
- Metropolitan Police Service

AIPAS pursues three objectives:

1. **Operational objective:** improve the knowledge and capabilities of UK LEAs and actors in the policing and security domain more broadly, on how to integrate AI accountability into their design, procurement and deployment decision-making and how to assess that specific AI capabilities and uses adhere to AI accountability principles
2. **Policy-related objective:** support policy-making and governance bodies with a mature, tested and (expert and citizen) validated definition of AI accountability for policing and security for formulating concrete legal and regulatory requirements to integrate AI accountability into sector-specific guidance
3. **Societal objective**: improve participation of society in the discussions and decision-making about AI use for policing and security purposes as integral part of AI accountability procedures, as well as increase societal awareness of AI accountability requirements and procedures

For more information, visit the AIPAS website: aipas.co.uk

The project is supported by the Engineering and Physical Sciences Research Council [Responsible AI IA091 Grant Ref: EP/Y009800/1]

Authors of the guidance: Prof. Babak Akhgar OBE; Prof. P. Saskia Bayerl; Prof. Fraser Sampson; Dr. Helen Gibson; Martin Snowden QPM; Chris Rowley KPM; Alexander Paradise; Christopher Spencer, Prof. John Parkinson OBE

Graphic design: Helen Grantham

Recommended citation: Akhgar, B., Bayerl, P.S., Sampson, F., Gibson, H., Snowden, M., Rowley, C., Paradise, A., Spencer, C., and Parkinson, J (2025). Guidance for Implementing AI Accountability in Policing. AIPAS/CENTRIC Report.

ISBN: 978-1-0369-2123-1

This work is supported by the Engineering and Physical Sciences Research Council [Responsible AI IA091 Grant Ref: EP/Y009800/1].