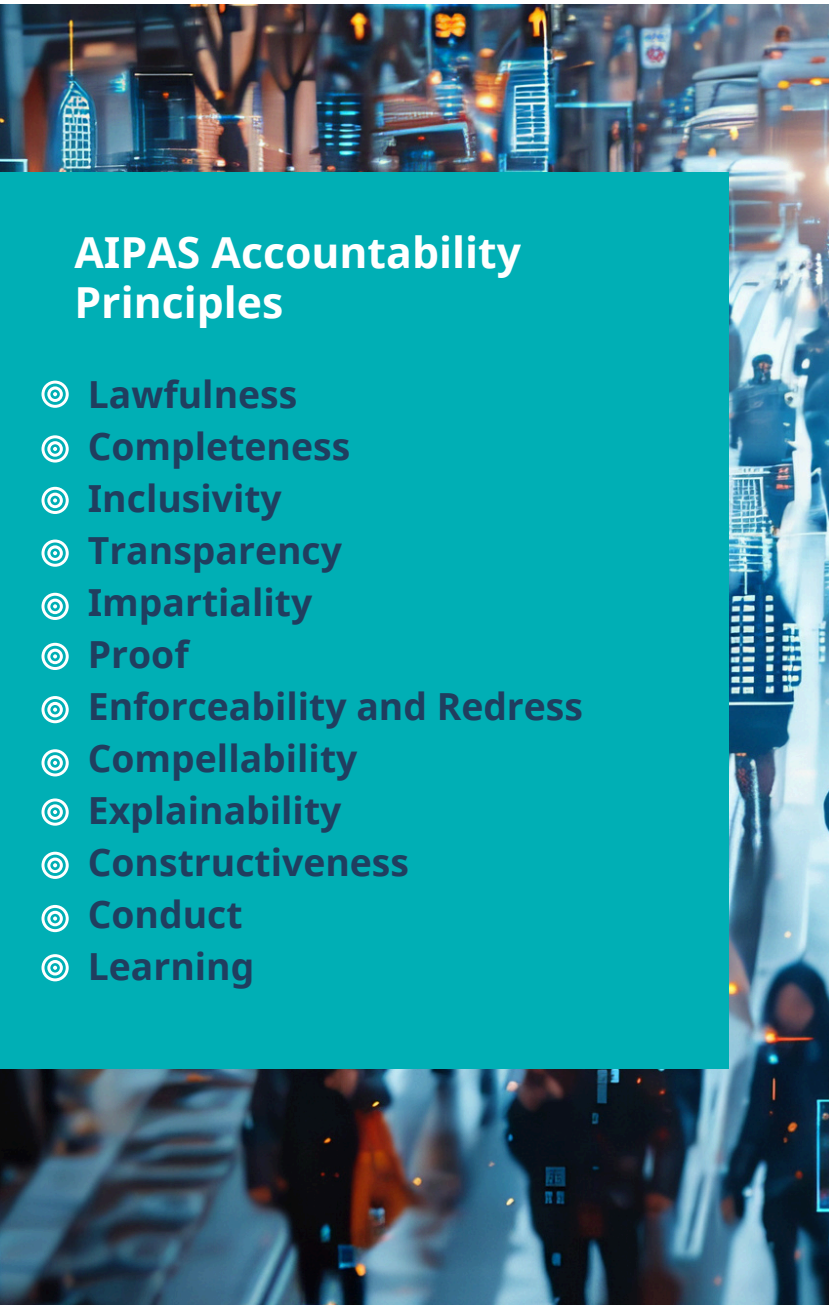
AI Accountability

AIPAS

for Policing and Security

Law Enforcement Agencies (LEAs) must balance the significant opportunities AI presents for safeguarding society with societal expectations about its responsible use. The AIPAS project designs practical mechanisms and a software tool for UK LEAs to assess and implement AI application accountability.

As AI continues to evolve within the law enforcement landscape, it is vital to assess how policy and governance can promote its ethical and responsible use. This factsheet outlines the AIPAS **12 key Accountability Principles** for AI deployments in law enforcement.



AIPAS Accountability Principles

- Lawfulness
- Completeness
- Inclusivity
- Transparency
- Impartiality
- Proof
- Enforceability and Redress
- Compellability
- Explainability
- Constructiveness
- Conduct
- Learning

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 accountability requires compliance with international, national and local laws. Lawfulness includes compliance with specific legal requirements such as the EU AI Act (where applicable) 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

Accountability arrangements must cover all relevant aspects of AI deployments, including partners and sub-contractors. This Principle effectively extends the reach of the 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 accountability arrangements (such as areas not expressly covered by the law), the protection and promotion of fundamental rights and freedoms should prevail.

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

Inclusivity - Leave no one out

Oversight must involve all relevant stakeholders engaged in and affected by a specific AI 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.

Impartiality - Empower independence

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 accountability mechanisms for AI systems should have a degree of independence from the line management structure of those involved in their design, development, supply and deployment. This applies in a personal, political, financial and functional way; any conflict of interest must be identified and addressed.

Transparency - Be open

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 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 accountability arrangements.

Proof - Follow the evidence

Law enforcement bodies are very familiar with capturing, analysing and presenting relevant, reliable evidence. 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.

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

Enforceability and Redress - **Make it right**

Without a 'so what?' element, accountability will be heavily diluted. For it to be meaningful to stakeholders, accountability must be underpinned by mechanisms giving people an effective remedy. These will include external legal and procedural routes for complaint and challenge but 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 accountability.

Compellability - **Make it work**

Closely linked to Enforceability and Redress, this Principle means oversight bodies must be in position to make the 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 accountability process. Linked closely with Enforceability and Redress, this Principle will be supported by contracts and Data Sharing Agreements.

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.

Constructiveness - **Aim for better**

Accountability is more than criticism. This Principle means all stakeholders participating 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.

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

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 European Code of Police Ethics states, "the condition of a democracy can often be determined just by examining the conduct of its police" and the expectations of individuals or organisations involved in AI systems should be expressly identified in advance. In this respect the approach may vary according to the country or agency involved, ranging from internal complaints handling, dispute resolution and mediation frameworks, to formal professional proceedings before courts or tribunals.

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 internal security 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.

AI Accountability
AIPAS
for Policing and Security

aipas.co.uk
aipas@shu.ac.uk
@aipas-uk

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