Leicestershire Police

Artificial Intelligence Policy & Procedure

Owner:	Head of Corporate Services
Department Responsible:	Corporate Services
Chief Officer Approval:	Deputy Chief Constable
Date of next review:	29/04/2027
Security Marking:	**Official**

This policy and procedure has been reviewed against APP and all relevant procedures.

Moved to APP:	N/A
Rationale:	N/A

This document has been produced in conjunction with the Leicestershire Police Legislative Compliance Pack

Review log

Date	Minor / Major / No change	Section	Author
21/10/2025	Creation	All	S40(2) S40(2) S40(2)
27/04/2026	Major	Appendix A, B & C Sections 4.3, 5.2,5.6,5.7	S40(2)

Note: Authorised Professional Practice (APP) has been checked.

Contents

1. Statement of Purpose 3

2. Scope 3

3. What is Artificial Intelligence? 4

3.1 Wider Definitions 5

4. AI Deployment Types 6

4.1 Integrated AI Tools 6
4.2 Standalone AI Tools 7
4.3 New AI Tools 7

5. Using AI 8

5.1 Intended uses of AI tools at Leicestershire Police 8
5.2 Environmental Consideration when using AI 9
5.3 Prohibited Information Types 9
5.4 What should I consider when using AI? 10
5.5 AI use in the Criminal Justice System 11
5.6 AI and Unused Material 12
5.7 Key Risks of Using AI in Policing 12
5.8 Expectations when using AI 13
5.9 Confirmation Bias 14

6. Roles and Responsibilities 14

7. Equality Impact Assessment 15

8. Appendix A – AI Implementation Plan 17

9. Appendix B – Force Approved Agent Governance Route 18

10. Appendix C – Agent Validation Checklist 19

1. Statement of Purpose

Artificial Intelligence (AI) technologies are increasingly being adopted across policing to enhance the delivery of services. When implemented safely, ethically, and appropriately, AI can significantly improve how we manage and analyse data, and how we communicate with and support the public, staff, third-party partners, and suppliers.

Leicestershire Police have established this document to provide clear direction on the responsible use of AI technologies. It aims to ensure that all deployments of this technology are subject to robust oversight and risk management processes, in line with legal, ethical, and operational standards.

The use of AI in the Force can broadly be split into three capability areas:

- AI supporting organisation effectiveness and efficiency
- AI supporting operational effectiveness and efficiency
- AI supporting individual decision making and expediting processes

This document also outlines the governance process that must be followed prior to the deployment of any AI technology within the Force. It also establishes the key principles that will regulate the use of AI throughout its lifecycle, ensuring transparency, accountability, and alignment with the Force's values and strategic objectives.

The adoption of AI within the policing community is considered a collaborative effort, with guidance and standards published by a number of sources. The following represent a non-exhaustive list of supplementary material which also should be considered when introducing a new AI related technology into the Force's environment:

- NPCC Cyber Standard – Artificial Intelligence
- NPCC Cyber Standard - Artificial Intelligence Large Language Models
- NPCC Cyber Standard - Artificial Intelligence Risk Assessment
- NPCC Covenant for Using Artificial Intelligence (AI) in Policing
- NPCC Artificial Intelligence (AI) Strategy
- NPCC AI Play Book
- UK Governments Responsible AI Toolkit
- UK Government Code of Practice for the Cyber Security of AI

The rapid nature of the development and application of AI is such that this document will be subject to regular review. Due to this, it is important to note that certain applications of the use of AI within the Force, especially if it is found to be being misused or considered to bring the Force into disrepute can be revoked at any time by the Force Senior Information Risk Owner (SIRO), a role held by the Deputy Chief Constable.

2. Scope

The Chief Constable has overall direction and control of Leicestershire Police and is ultimately accountable for all policies and supporting documents of the organisation

and its actions. Adherence to this force policy will be expected from: all Officers, Special Constables, Police Staff, Police Support Volunteer, Contractors, agency staff and any other individual provided access to the Force's IT environment.

In accordance with this document, it is the duty of all staff to ensure that any usage of AI is done so in a manner that promotes fairness and avoids bias and continues to align with the Forces values and ethical standards.

3. What is Artificial Intelligence?

There is currently no universally accepted legal definition of Artificial Intelligence (AI). The Alan Turing Institute (2021) acknowledges that AI is often used as an umbrella term encompassing related technologies such as automation, neural networks, and machine learning. For clarity and consistency within policing, Leicestershire Police adopts the following working definitions, aligning with the definitions utilised by the National Police Chiefs' Council (NPCC) and the Police Digital Service. Additionally, practical examples of each definition have been provided to assist the reader.

- **Artificial Intelligence (AI)** refers to a machine or system that learns, generalises, or infers meaning from input data, thereby reproducing or surpassing human performance. This includes tasks such as image analysis to detect illegal content or predictive modelling for operational planning. AI may also refer more loosely to systems capable of performing repetitive tasks without human guidance.

An example of this type of AI would be a system that analyses CCTV footage, to determine if it contains illegal activities such as child sexual abuse, without the need for human intervention to review the footage.

- **Machine Learning (ML)** is a subset of AI involving algorithms that improve their performance over time by learning from new data, without being explicitly programmed. ML underpins many modern policing tools, including speech recognition, fraud detection, and behavioural analytics.

An example of ML is a fraud detection tool that becomes more accurate as it learns from patterns in previous financial crimes.

- **Advanced Data Analytics (ADA)** involves the use of specialised techniques and subject matter expertise to extract insights from complex datasets. ADA goes beyond traditional business intelligence and may include methods such as Risk Terrain Modelling, linear regression, and language analytics to support strategic decision-making.

An example of ADA is a hotspot in policing tool which identifies areas with higher likelihood of crime based on environmental factors, guiding where officers should be deployed.

There are other related AI terminology, which start to overlap with the above, but are included here for completeness. The above and below are considered the most common, but there are others. The additional definitions are

- **Generative Artificial Intelligence (GAI)** refers to AI systems capable of creating new content—such as text, images, or audio—based on patterns learned from training data. These models are increasingly used in investigative and administrative contexts, such as automated report drafting or evidence summarisation.

- **Large Language Models (LLMs)** are a subset of GAI trained on vast amounts of text data, enabling them to generate human-like responses and perform tasks such as translation, summarisation, and conversational interaction. Examples include ChatGPT and Google Bard, to summarise lengthy policy documents or assist with drafting emails.

- **Natural Language Processing (NLP)** is the branch of AI focused on enabling machines to understand and interpret human language. NLP is used in tools that transcribe interviews, analyse sentiment, and extract key information from documents.

Overall, the term "AI" has ultimately been adopted as an umbrella term that has encompassed various forms of technology. All users of this framework must be alive to the fact that AI technology is not always visible, especially where it forms part of a background function incorporated into an application or similar tool.

Please note: Despite any terminology utilised for the naming of a type of an AI, this document is considered to be applicable to ALL types of AI regardless of their application. Should any doubt arise, please contact the IT Service Desk or Information Security team for further advice.

3.1 Wider Definitions

The following table provides a glossary of terms which may also be referenced within this document:

CHIS (Covert Human Intelligence Source)	A person who provides information to the police in secret, often about criminal activity.
Copilot	Microsoft's AI tool approved for use in Leicestershire Police, integrated into Microsoft 365 applications
DPO (Data Protection Officer)	DPO (Data Protection Officer) – The person responsible for ensuring Leicestershire Police follows data protection laws and handles personal data properly.
MOPI (Management of Police Information)	National guidance on how police information should be handled, stored, and shared.
SIRO	Senior Information Risk Owner. A role held by the Deputy Chief Constable within

	the Force. The SIRO is an executive who is familiar with information risks and understands how the strategic business goals of the organisation may be affected by failures in the security of an Information System. Overall, they lead on the Force response to risk, and as such set the Force appetite to information risk and act as the advocate for information risk on relevant boards and internal discussions.
Special Category Personal Data	Sensitive personal information such as race, religion, health, or sexual orientation, which requires extra protection.

4. AI Deployment Types

Leicestershire Police currently deploy Artificial Intelligence (AI) technologies in two primary forms.

4.1 Integrated AI Tools

Integrated AI refers to AI capabilities embedded within the existing platforms and systems used across the Force. These features are often part of commercial or operational software, and its use may not be overtly visible to users. Examples include:

- **Automated redaction tools** within document management systems.
- **Facial recognition features** embedded in digital evidence platforms.
- **Microsoft's embedding of Co-Pilot** within the Microsoft Office Suite of products

These technologies are increasingly common across public sector services and are adopted to enhance efficiency, accuracy, and data handling practices. All integrated AI deployments are subject to a specific risk assessment process, led by the Information Management department in collaboration with key stakeholders such as IT and Procurement. For AI deployments of this nature, each AI feature is evaluated for:

- **Appropriateness of use** within the policing context.
- **Technical Safeguards** to protect sensitive Force data.
- **Compliance** with legal, ethical, and operational standards.

It is not the intention of this document to provide a comprehensive list of all integrated AI tools authorised for use in Force, however key examples of Integrated AI tools within the Force include:

- Nice Investigate – The Force's Digital Evidence Management solution
- GoodSam – A tool for communicating with the public
- Riven DocDefender – A tool for redacting documents

These examples provide a practical example of the Force's three capability areas for the use of AI, as each application seeks to introduce efficiency savings in a secure manner.

4.2 Standalone AI Tools

Standalone AI tools refer to applications where the AI model is directly accessible to the user as its own application, rather than as part of another system. These tools are most commonly of the Generative AI type allowing users to upload Force data and interact with the model via prompts—for example, asking the AI to analyse an Excel spreadsheet or summarise a document.

Like Integrated AI, all standalone AI tools are subject to a specific risk assessment process led by the Information Management team, in collaboration with stakeholders such as IT and Procurement. However, due to their extensive capabilities and potential for uncontrolled data processing, these tools present a heightened risk and are therefore subject to strict regulation within policing, with stakeholders such as the Police Digital Service providing additional guidance to the Force for their safe deployment.

S24(2), S31(3)

S24(2), S31(3)

No other standalone AI tools may be used within the Force. This includes, but is not limited to, the following prohibited commercial AI tools:

- Microsoft Copilot (Consumer/Personal versions)
- ChatGPT
- Deepseek
- Gemini
- Perplexity
- Self-hosted, either on-premises or cloud based, LLM's or generative AI tool such as open-source models.
- AI tools integrated into existing products where they are not explicitly authorised in section 5.1
- Any other commercially available Large Language Model (LLM) or Generative AI tool

4.3 New AI Tools

Integrated AI tools that are part of a wider product being adopted do not require endorsement by the Productivity and Efficiency Board, as their procurement route will already include an evaluation of the AI tooling.

The use of new standalone AI tools must be approved by the Productivity and Efficiency Board, alongside any other governance required for that product (such as procurement, information security, information management etc). The AI Working group should be consulted for all new AI initiatives.

The Board will consider the tools compliance in respect of this policy and any national guidance, alongside the ethics of its use and any steps taken by the tool or intended users to mitigate any identified risks.

New AI tools will be considered within the three following 'buckets':

- **Prompted AI** – Tools that require direct user input, such as CoPilot Chat, to interact with.

- **No-code or low-code AI** – Tools that allow automation using AI, such as CoPilot Studio or Power Automate using AI connectors. These tools allow AI to be used within automated workflows, whether or not they require human input at some stage. Workflows are usually designed in a visual interface and require no, or minimal, code.

- **Coded AI** – Tools that require custom development to implement, such as a Python script that connects to a database via an API and processes the data through an LLM model.

The governance process in respect of gaining authorisation for the use of new AI tools is contained within Annex A. The process differs depending on the 'bucket' of tool intended to be used, as the risks associated with each 'bucket' are different.

5. Using AI

5.1 Intended uses of AI tools at Leicestershire Police

Artificial Intelligence (AI) presents significant opportunities for modern policing. From enhancing operational efficiency and improving decision-making to supporting frontline officers and streamlining administrative tasks, AI technologies can deliver real-world benefits across the Force. Leicestershire Police recognises the value of innovation and is committed to enabling the safe and responsible adoption of AI.

AI is intended for use in the following types of activities within Leicestershire Police.



[redacted]
S24(2) &23(3)

5.2 Environmental Consideration when using AI

Users must also consider the environmental impact of using artificial intelligence. AI systems require significant computational power, which in turn consumes electricity and water for data processing and cooling of data centres. While AI can offer efficiency and productivity benefits, unnecessary or excessive use of AI should be avoided, and users are expected to employ AI tools responsibly and sensibly, balancing potential benefits against environmental and sustainability considerations.

5.3 Prohibited Information Types

[redacted]
S24(2) & 23(3)

[redacted]
S24(2) & 23(3)

[redacted]

Guiding Principle: If you are unsure whether a piece of information is suitable for use in Copilot Chat, **do not input it.** Always steer on the side of caution. Seek the advice of your line manager or the Force's Information Security team first.

5.4 What should I consider when using AI?

The use of AI and in policing is relatively new. It is complex technology that appears to have obvious and immediate benefits across a range of policing activities so it is likely that officers and staff of all ranks and roles will quickly experiment and adopt its use with well-founded good intentions.

However, there are number of risks that are real, likely to occur and have the potential to have a high impact on individuals and public confidence in policing. Users are therefore expected to be cautious and professional. Although the below section will highlight several benefits and risk associated with the use of LLM's, there are a few simple steps that users can take to significantly reduce the risks of using generative AI.

1. **Only use AI tools that are authorised –** (see Approved AI above)

2. **Always ensure you're using a force account on a force device –** the use of personal accounts is prohibited. No policing data should **ever** be put into AI on a personal device or account. Only AI authorised by this policy can be used, when logged in using your police account on a work device. For example, using a personal mobile phone with an AI-powered transcription app to record and transcribe a meeting, interview, or operational briefing is strictly prohibited. Such actions risk unauthorised data exposure and breach of Force policy.

3. **Think before use –** is the use of AI in this case, sensible, appropriate and ethical?

3. **Protect our data –** keep personal information secure, and out of the AI unless absolutely necessary.

4. **Check the results –** AI is not 100% reliable and you must always read and verify anything produced. AI Models, Including LLM's , can sometimes 'hallucinate'—this means they may generate information that sounds plausible but is actually incorrect, made up, or not supported by real data. These hallucinations can include invented facts, inaccurate details, or even entirely fictional references. It's important to verify AI-generated content, especially when accuracy is critical

5. **Be transparent –** Don't claim AI produced work as your own. Although there is no need to declare every use of AI such as for note taking, drafting work you heavily edit or for research, transparency is essential to maintain the public trust so always declare the use of AI in any formal report, creative content or when it is used in decision making. Use a note such as, "*Microsoft Copilot supported the creation of this document".*

6. **Human Review –** AI must not be allowed to make operational decisions without human review. AI can be used as a tool, to present options and wider considerations. However, the responsibility and liability remain with the police decision maker. AI can never be used as a defence or rationale for a poor decision.

6. **Report any concerns –** raise any concerns, mistakes or breaches as soon as possible with your supervisor or the Data Protection team. The sooner they know about issues the sooner they can mitigate the impact.

7. **Maintain Professional Standards** - Use AI in a way that upholds the integrity and professionalism expected in the police service.

8. **Comply with the Force's wider Policies and Procedures -** A non-comprehensive list includes:

   - Standards of Professional Behaviour – Police Officers
   - Standards of Professional Behaviour – Police Staff
   - Information Management Policy
   - Information Security Policy and Procedure.
   - Internet Access and Social Networking Procedure
   - The National Code of Ethics
   - The Management of Police Information (MoPI) framework
   - All relevant Data Protection legislation including the UK GDPR and the Data Protection Act 2018.

9. **Avoid Bias and Harm** - Be alert to potential bias, stereotyping, or inappropriate content in Copilot outputs. Report any concerning outputs to your supervisor

5.5 AI use in the Criminal Justice System

S24(2) & 23(3)

However, AI may be used to support investigators in understanding evidence or assisting with the investigative process, provided it is not involved in the generation of any official evidential documentation.

Where AI has been used for internal efficiencies or benefits, for example to help write a entry for an OEL log on NICHE, then the use of AI must be disclosed.

[redacted]
S24(2) & 23(3)

5.6 AI and Unused Material

[redacted]
S24(2) & 23(3)
[redacted] it is acknowledged that AI may have been used in the investigation to help progress the case. As with any material generated as part of an investigation, it must be retained and disclosed on the disclosure schedules and accurately described to include that AI has been used to assist in drafting the material. Investigators should retain all original information inputted, the prompt used and software used to generate the material.

Important note – AI generated content must be checked as carefully as if you wrote it yourself – the author is responsible for the final content.

5.7 Key Risks of Using AI in Policing

While Artificial Intelligence (AI) offers significant potential to enhance policing operations, it also introduces a range of risks that must be carefully managed. The following outlines key areas of concern and the associated mitigations in place within Leicestershire Police:

- **Bias and Stereotyping**

  AI systems may reflect or amplify societal biases present in their training data. This can result in unintended reinforcement of stereotypes related to gender, race, profession, or other protected characteristics.
  Mitigation: Approved AI tools undergo bias testing and ethical review, but it is acknowledged that not all harmful content can be fully prevented.

- **Overrepresentation or Underrepresentation**

  Certain groups may be disproportionately represented—or excluded—in AI-generated outputs. For example, legitimate content relating to LGBTQIA+ topics may be filtered or misrepresented.
  Mitigation: Microsoft and other vendors apply classifiers and prompt engineering techniques to reduce this risk, but users must remain vigilant.

- **Inappropriate or Offensive Content**

  AI may generate content that is offensive, controversial, or inappropriate, including text, images, or audio containing harmful symbols, language, or themes.
  Mitigation: Safeguards and content filters are in place, but some material may still bypass these controls. Users must report any concerning outputs immediately.

- **Information Reliability**

  AI tools can produce inaccurate, misleading, or fabricated information—commonly referred to as "hallucinations." This includes misrepresentation of facts, sources, or context.
  Mitigation: Users must verify all AI-generated content before acting on it, especially where operational or evidential decisions are involved.

- **Multilingual Performance**

  AI systems used within the Force are optimised for English. Performance in other languages may be less accurate or fluent, potentially affecting usability and interpretation.
  Mitigation: Where multilingual support is required, human review and translation should be used to validate outputs.

- **Audio Input Limitations**

  Voice-based AI tools may struggle with background noise, regional accents, or unclear speech, leading to transcription errors or misinterpretation.
  Mitigation: Use in controlled environments is recommended, and manual review of transcriptions is required.

- **Internet Dependence**

  Most AI tools rely on a stable internet connection. Connectivity issues can disrupt access, reduce performance, or cause data loss.
  Mitigation: Users should ensure secure and reliable network access when using AI tools, and avoid using them in offline or unstable environments.

5.8 Expectations when using AI

The use of AI tools must always take place in accordance with the Code of Ethics, Data Protection Laws and the force values. Specific guidance is provided to assist users in making sound decisions:

1. Use Responsibly and Ethically
- Use AI in line with legislation and policy.
- AI should support, not replace, professional judgment, especially in sensitive situations.

2. Protect Confidentiality
- S24(2) & 23(3)
- Follow all data handling and information security policies.
- All outputs generated by AI tools used in official documentation must be stored in accordance with MOPI and Leicestershire Police's data retention policies.

3. Be Transparent When Required
- Declare when AI has been used in formal reports, public documents, or decision-making.
- Ensure all outputs are reviewed and clearly attributed.

4. Verify and Validate Outputs
- Always fact-check and assess AI-generated content.

- Users are responsible for the accuracy and appropriateness of any content they use.

5. Avoid Bias and Harm

- Be alert to potential bias, stereotyping, or inappropriate content in AI outputs.
- Report any concerning outputs to your supervisor.

6. Stay Within intended Use Cases

- Use Copilot only for appropriate tasks (e.g., drafting, summarising, research support).
- Do not use it for legal interpretation, risk assessments, or direct public communication without review.

5.9 Confirmation Bias

Confirmation bias can subtly influence how officers and staff prompt and interpret AI outputs, much like how leading a witness can unintentionally shape their account. For example, prompting an AI with a predetermined outcome—such as *"We need grounds to justify refusing this procession application, what reasons can we use?"*—pushes the system toward supporting that conclusion. A neutral alternative like *"Summarise all relevant risks and safeguarding considerations associated with this planned procession"* allows a more balanced assessment. This reflects the wider investigative risk identified in policing guidance, where officers can naturally favour information that reinforces their initial hypothesis and are therefore encouraged to "consider the opposite" to maintain objectivity. Likewise, when AI is used to produce operational briefings, prompts framed around assumed disorder or threat can unintentionally reinforce untested narratives. Force policy on AI reiterates that systems may amplify existing bias, requiring officers to construct neutral prompts, verify outputs, and ensure impartiality.

6. Roles and Responsibilities

- **Governance**

  The governance procedure for all new AI ideas is outlined above. Consultation with key stakeholders should be sought before submission (IT, Information Management, Information Security etc). If the implementation of the new AI product comes with increased expenses, it will then go to the Force Executive Board for final sign off.

- **Artificial Intelligence Board**

  Responsible for commissioning new AI ideas and authorising new trials, and project progression into 'business as usual'.

- **Executive Board**

  Responsible for authorising any additional expenditure in relation to developing AI or New AI Products.

- **Digital Board**

  Monitoring the use of AI will be covered by the Digital Board.

- **Strategic Lead**
  - Oversees the development, review, and communication of the AI policy.
  - Ensures policy compliance across the force and coordinates updates in response to legal, technological, or operational changes.
  - Liaises with national bodies and internal stakeholders to align with best practices.

- **Data Protection Officer (DPO)**
  - Provides guidance on data protection compliance in relation to AI use.
  - Reviews reported incidents or breaches involving AI tools.
  - Supports risk assessments and data protection impact assessments (DPIAs) where applicable.

- **Line Managers / Supervisors**
  - Ensure their teams understand and comply with the policy.
  - Act as the first point of contact for questions or concerns about AI use.
  - Escalate any misuse or incidents to the DPO or Strategic Lead.

- **IT and Digital Services Team**
  - Manages access to authorised AI tools (e.g., Microsoft Copilot).
  - Ensures technical safeguards are in place to prevent unauthorised use.
  - Monitors system usage and supports secure integration of AI tools.

- **All Leicestershire Police Staff and Officers**
  - Use only authorised AI tools in accordance with this policy.
  - Avoid inputting prohibited or sensitive information into AI systems.
  - Verify AI-generated content before use and maintain transparency in formal outputs.
  - Report any concerns, errors, or breaches promptly to their supervisor or the DPO.

- **Training (Team Leicestershire Academy)**
  - Develops and delivers training on responsible AI use.
  - Ensures staff are aware of the risks, benefits, and ethical considerations of generative AI.

7. Equality Impact Assessment

Leicestershire Police places trust in their employees to comply with force policies and to work in accordance with and in support of:

Leicestershire Policing Pledge
Code of Ethics | College of Policing

This policy has been developed with consideration for the potential risks and benefits of generative AI use across all protected characteristics. It aims to prevent discrimination, promote equality of opportunity, and foster good relations by ensuring responsible and ethical use of AI tools.

	What impact has this policy **had**	How **will** this updated policy

	on the nine protected characteristics in relation to the three general duties? (If applicable)	positively impact each of the nine protected characteristics in relation to the three general duties? If not, explain why it will not.
Age (including children and young persons)	No negative impact identified. The policy applies equally to all age groups.	Promotes inclusive use of AI tools and ensures outputs do not discriminate based on age. Encourages review of content to avoid age-related bias.
Disability	No adverse impact identified. AI tools may support accessibility.	Supports productivity for staff with disabilities through features like summarisation and drafting. Encourages review to avoid discriminatory content.
Gender Reassignment	No negative impact identified. Policy prohibits discriminatory or biased outputs.	Reinforces respectful and inclusive language. Promotes awareness of potential bias in AI-generated content.
Pregnancy & Maternity	No direct impact identified. Policy ensures sensitive data is protected.	Prevents misuse of AI in ways that could expose or mishandle personal data related to pregnancy or maternity.
Marriage & Civil Partnership	No direct impact identified.	Ensures AI tools are not used in ways that could lead to discrimination based on marital or partnership status.
Race	Recognises the risk of racial bias in AI outputs.	Promotes vigilance and correction of racially biased content. Supports equality by requiring review and transparency.
Religion or Belief	No negative impact identified.	Encourages sensitivity in AI-generated content and prohibits offensive or inappropriate outputs.
Sex	Acknowledges potential for gender bias in AI tools.	Promotes fair representation and requires users to identify and correct biased outputs.
Sexual Orientation	Recognises risk of underrepresentation or misrepresentation.	Supports inclusion by requiring users to report and address biased or inaccurate content related to LGBTQIA+ topics.

8. Appendix A – AI Implementation Plan

Type of AI Application	Explanation / Examples	Governance
	**Bucket 1 – Prompted AI** Prompted AI refers to tools that require direct user input to function. Users craft prompts or instructions, and the AI generates outputs such as text, images, or analysis. It relies on human guidance, ensuring control while enhancing productivity **Examples: Co-Pilot Chat, GoodSAM Transcriptions**	**<u>Self-Governance</u>** With consideration and compliance with: • Force AI Policy • Force Policy and Procedures • Information Security • Code of Ethics • Standards of Professional Behaviour
	**Bucket 2 - Workflow Agents – (No Code / low code)** Workflow agents are AI-driven tools that automate and streamline tasks within a process. They follow predefined logic, perform actions across systems, and support staff by handling repetitive steps. Designed to improve efficiency and consistency, they enhance business workflows without requiring direct user prompting **Examples: Self Triggered AI Audit Tools**	**<u>Streamlined Governance Procedure</u>** • Head of Directorate Approves use of AI to resolve the problem. • Problem statement endorsed agreed at Productivity and Efficiency board • Corp Services Validation (including Information security, Info Management and other key stakeholders) • Sign off by C/Insp Corp Services • Deployment decision - P&E Board.
	**Bucket 3 – Coded AI** Coded AI refers to solutions built through custom development. Developers write code—such as Python scripts or API integrations—to process data and interact with AI models. It enables highly tailored automation and advanced capabilities but requires technical expertise to design, deploy, and maintain. **Examples – Agentic AI**	**<u>Full Governance Procedure</u>** • Information Management • Information Security • DPIA and EIA • IT Consultation • AI Working Group • PMO Consultation • Layer Board Sign off • SIRO Sign Off • Paper for Sign off at Exec Board

9. Appendix B – Force Approved Agent Governance Route



10. Appendix C – Agent Validation Checklist

1. Purpose & Business Justification

Checklist item	Yes / No / N/A	Free-text comments / evidence
The business problem the agent addresses is clearly defined		
There is a stated operational or corporate benefit (time saving, quality, consistency, compliance)		
The agent does not duplicate existing approved tools or processes		
Use of AI is proportionate to the problem being solved		
There is clarity on whether AI is assisting or automating decision-making		
A named business owner / SRO is accountable for the agent		

2. Scope & Intended Use

Checklist item	Yes / No / N/A	Free-text comments / evidence
The agent's intended users are clearly defined (role-based, not generic)		
Use cases are explicitly described (what it can and cannot be used for)		
The agent does not create court ready documents or make operational decisions		
Outputs are advisory, draft, or assistive only		
Clear instructions exist requiring human review before outputs are relied upon and a reporting mechanism is included for identified issues or errors once deployed.		

3. Data Protection & Information Management

Checklist item	Yes / No / N/A	Free-text comments / evidence
Data inputs are clearly documented		
No prohibited data types are being processed (e.g. CHIS, legally privileged material, covert data)		
If the agent processes personal data, inputs and outputs comply with DPA 2018 and UK GDPR principles		
Data minimisation is applied (only necessary data is used)		
There is no onward sharing of data to external services or plugins		
Retention and deletion considerations have been assessed in line with the Force's retention schedule		
If the agent processes personal data, it is not programmed to leverage this in a way that is incompatible with the original purpose for processing		

4. Information Security

Checklist item	Yes / No / N/A	Free-text comments / evidence
No data above approved handling level is used		
Agent has been risk assessed and signed off by Information Security – and agent has passed their risk assessment and matrix.		
No external APIs, connectors, or unmanaged integrations are used		
Role-based access controls are in place		
Sharing of the agent is restricted and controlled (IT)		
No system credentials, passwords, or tokens are embedded		
Security logging and auditability are understood		

5. Ethics, Legality & AI Risk

Checklist item	Yes / No / N/A	Free-text comments / evidence
IS the agent compliant with the Code of Ethics		
Are the knowledge sources from reliable sources?		
Risks of bias, over-reliance, hallucination, or misinterpretation have been considered		
Clear caveats are presented to users about accuracy and limitations		
Agent does not profile individuals or predict risk without lawful basis		
No automated decision-making that produces legal or operational outcomes		
Human accountability is clearly retained		
Is the agent compliant with the AI checklist?		

6. Transparency & Explainability

Checklist item	Yes / No / N/A	Free-text comments / evidence
Users are informed they are interacting with an AI agent		
The agent's purpose and limitations are clearly described		
Prompts, logic, and content sources are documented		
Users understand outputs may be incorrect or incomplete		
Outputs are not presented as authoritative or definitive		

7. Quality Assurance & Testing

Checklist item	Yes / No / N/A	Free-text comments / evidence
Tested with realistic scenarios		

Known failure modes and limitations are documented		
Outputs reviewed by a subject-matter expert		
Testing includes edge cases and misuse scenarios		
Mechanism exists for users to report issues or errors		
QA or dip-sampling arrangements are defined (if applicable)		

8. Governance, Ownership & Change Control

Checklist item	Yes / No / N/A	Free-text comments / evidence
Named technical owner and business owner recorded		
Version control / change log exists for prompts and logic		
Clarity on who can amend, retire, or disable the agent		
Alignment with force AI policy and governance framework		
Approval authority (directorate / board) documented		

9. Training & User Readiness

Checklist item	Yes / No / N/A	Free-text comments / evidence
Users receive guidance on appropriate use		
Instructions reinforce that AI outputs must be checked		
Misuse risks are explicitly addressed		

10. Monitoring, Review & Exit Strategy

Checklist item	Yes / No / N/A	Free-text comments / evidence
Usage can be monitored at an appropriate level		
Planned review point after deployment		
Metrics or qualitative feedback will be captured (benefits)		
Clear route to withdraw the agent if issues arise		

Final Approval Summary

Decision	Yes / No	Free-text reasons / conditions
Suitable for deployment		
Suitable with conditions		
Not suitable		

Approving authority:

Date:

Review date: