ABOUT THIS POLICY

The aim of this Policy is to ensure that appropriate use, considerations and risks are considered when looking to implement AI technologies for force purposes.

TITLE	Joint Artificial Intelligence: Acceptable Use Policy
DEPARTMENT RESPONSIBLE	Information Governance/Information Security
DATE CREATED	29/01/2026
LAST FULL REVIEW	29/01/2026
LAST EDITED	29/01/2026
NEXT REVIEW DATE	29/01/2027
VERSION	V1
SECURITY CLASSIFICATION	Official
EXTERNAL PUBLICATION	Yes
COLLEGE OF POLICING APP	Data Driven Technologies APP
KEY SEARCH TERMS	Artificial Intelligence AI Acceptable Use AI Governance Responsible AI Ethical AI Human Oversight Explainability Accountability Transparency AI Agents Automation Data Protection UK GDPR Data Protection Impact Assessment (DPIA) Personal Data Special Category Data Human Rights Act Equality Act Freedom of Information ICO AI Guidance Third-Party AI Supplier Assurance AI Procurement Cloud AI Services Data Residency ISO/IEC 27001:2022 AI in Policing NPCC AI Covenant NPCC AI Strategy AI Playbook for Policing Data Driven Technologies Operational Policing Technology AI Risk Management Bias and Fairness Accuracy Content Verification Hallucinations Misuse of AI Prohibited AI Use Monitoring and Audit Disciplinary Action AI Standards and Ethics Forum Change Approval Board (CAB) Service Improvement Board (SIB) Training and Awareness Approved AI Tools Cyber Essentials Plus Information Security Information Governance Official OFFICIAL SENSITIVE Data Classification Data Minimisation Secure Configuration Risk Assessment Information Asset Owner (IAO) Senior Information Risk Owner (SIRO) Generative AI Large Language Models (LLM) AI Platforms AI Toolkit User-Level AI Agents Admin-Level AI Agents Role-Based Access Control (RBAC) Secure AI Configuration AI Register Governance Boards ISO/IEC 42001

How to navigate this document:

You can either:

- Scroll through each page in sequence
- Or click on the tabs on the right-hand side to go to a specific section

If you have any questions on this policy, please email the Policy Unit

COPIES AVAILABLE IN WELSH. CONTACT POLICY UNIT: PolicyUnit@south-wales.police.uk

KEY POINTS

COPIES AVAILABLE IN WELSH. CONTACT POLICY UNIT: PolicyUnit@south-wales.police.uk

ROLES & RESPONSIBILITIES

Users

- Users must adhere to the contents of this policy and promptly report violations or security incidents involving AI technology to the Force Information Security Team

Business lead/Project Manager

- Submit business justification form to the AI / Automation Standards & Ethics Forum
- Conduct a Data Protection Impact Assessment
- Engage with the Information Governance /Force Information Security Officer/ICT/SRS/DSD
- Identify and consult with stakeholders/interested parties during the development of the proposal and document concerns/observations raised

Stakeholders/Interested parties

- Stakeholder and interested parties are required to be engaged and attend the AI / Automation Standards & Ethics Forum to review the scope of the AI use case.

Information Asset Owner

- Ensure any processing of data from information assets under their control are fully documented prior to project initiation.
- Ensure they agree with any processing activity involving their information asset
- Update any changes required to entries in their Information Asset Register with details of the processing

Procurement

- Where the processing involves the use of a third-party supplier(s), the process will need to be reflected in the instructions provided to them for the processing as part of the contract and supplier assurances will have to be provided to mitigate risks

Senior Information Risk Owner

- Where the processing carries a high risk, the senior information risk owner will be required to:

a) Terminate (Reject Risk)
b) Transfer (Share Risk)
c) Treat (Mitigate Risk)
d) Tolerate (Accept Risk)

DDAT Director

- Will chair the AI / Automation Standards and Ethics Forum

Information Governance

- Will oversee completion of Data Protection Impact Assessments and advise on relevant provisions for information sharing agreements or contracts
- Will maintain the AI Toolkit
- Will record information risks associated with force use of AI
- Will apply the ICO/NPCC/DSIT/College of Policing guidance on use of AI and data protection
- Liaise with other forces on data protection compliance with AI
- Will investigate and record any data incidents involving personal data and unauthorised use of AI.

ICT/SRS/DSD

- Ensure all technical information relating to AI technologies is documented.
- Personal AI Agents (User-Level): These are small AI tools that staff can use with their own data or within their team's applications. You can use these to help with tasks like summarising documents or analysing team data. They must not access wider organisational systems or sensitive data.
- Organisation-Wide AI Agents (Admin-Level): These are powerful AI tools that work across the whole organisation or connect to important systems. Only ICT, SRS, or DSD administrators are allowed to create or manage these. These agents can affect many users or access sensitive information, so they need strict controls. A full request must be submitted to the CAB or SIB in GWP, including what the AI will do and how risks will be managed.
- Ensure non approved AI technologies are restricted
- Responsible for the secure configuration of AI Assets.
- Vendors' patch release notes referencing "AI", "machine learning", "predictive", "LLM" must be reported to AI / Automation Standards & Ethics Forum before patch deployment.
- Technically apply the agreed AI standards and approved use

Information Security

- Conduct risk assessments on any AI proposals to ensure that the force security is not compromised.
- To maintain a register of approved AI tools and the purpose for which they are used.
- To continuously monitor the development of enhanced capabilities of such tools.

FULL POLICY

1. Purpose

This policy establishes the acceptable use, governance, and strategic adoption of Artificial Intelligence (AI) technologies within South Wales Police and/or Heddlu Gwent Police. It ensures that all AI deployments are lawful, ethical, secure, and aligned with operational and public service objectives.

Application of AI to force functions must be in accordance with NPCC AI Principles as set out in the NPCC AI Covenant , the NPCC AI Strategy, Data Protection laws, Information Security Principles and local policies and procedures.

All policies and procedures which apply to devices and information are relevant and should be considered alongside this document.

2. Scope

This policy applies to all employees, officers, contractors, volunteers, and third-party suppliers who interact with or deploy AI technologies in any capacity within South Wales Police and/or Heddlu Gwent Police and/or Heddlu Gwent Police.

3. General Principles

Lawfulness

AI technologies must comply with all applicable laws, including data protection, human rights, and equality legislation.

Transparency

AI use must be communicated clearly to stakeholders and the public, including its purpose, limitations, and safeguards.

Accountability

Users and developers are accountable for AI outputs and must ensure human oversight is maintained.

Explainability

AI systems should provide understandable outputs, especially when used in decision-making.

Robustness

AI tools must be tested for accuracy, fairness, and resilience against bias or misuse.

Ethical Use

AI must be used in ways that uphold public trust, avoid harm, and respect individual rights.

3.1. Industry Collaboration & Best Practice

South Wales Police and/or Heddlu Gwent Police and Heddlu Gwent Police recognises the importance of collaborating with industry partners to ensure the responsible and effective use of Artificial Intelligence technologies. All AI initiatives should seek to:

- Engage with reputable industry stakeholders to benefit from innovation, technical expertise, and ethical standards.
- Align with government-issued best practice and guidance, including frameworks such as the UK Government AI Playbook, NPCC AI Strategy, and relevant Parliamentary briefings.
- Ensure that any external partnerships uphold the force's legal, ethical, and operational standards, and are subject to appropriate governance, including DPIAs and Information Security assessments.

4. Acceptable Use of AI

4.1. Acceptable Use of AI

Only approved AI platforms may be used for designated tasks such as summarising documents, drafting templates, generating insights, and supporting research. All outputs must be reviewed by the user for accuracy, appropriateness, and compliance before use.

Examples of Acceptable Use of AI:

a) Summarising publicly available documents (e.g., government reports, academic papers).
b) Drafting generic templates for meeting agendas, project plans, or training schedules.
c) Creating PowerPoint structures for presentations on non-sensitive topics.
d) Generating Excel formulas to automate calculations or troubleshoot spreadsheet errors
e) Researching general knowledge topics (e.g., weather trends, construction methods, legislation summaries).
f) Improving grammar and clarity of non-sensitive communications (e.g., internal memos, newsletters).
g) Drafting first versions of non-sensitive reports (e.g., policy proposals, training outlines).
h) Creating productivity tools like checklists, calendars, or task trackers.
i) Finding academic references for professional development or training.
j) Describing IT issues more clearly for submission to the ICT Service Desk.

4.2. Unsanctioned Use of AI

Use of non-approved AI platforms, including consumer-grade or browser-based tools, is strictly prohibited. Users must not input personal data, operational details, or sensitive content into any AI system without prior approval.

AI must not be used to process personal, sensitive, or classified information such as OFFICIAL SENSITIVE unless explicitly authorised through formal governance channels.

4.3. Understanding "OFFICIAL SENSITIVE" Information

OFFICIAL SENSITIVE is a UK government classification used to describe information that, if disclosed inappropriately, could cause harm to individuals, operations, or the organisation. In a policing context, this includes:

Examples of OFFICIAL SENSITIVE Information:

a) Personal data about victims, suspects, or witnesses.
b) Details of ongoing investigations or intelligence operations.
c) Internal procedures, tactics, or surveillance methods.
d) IT system configurations, passwords, or vulnerabilities.
e) Legal advice or privileged communications.
f) Any data that could compromise public safety or operational integrity.

4.4. Why It Matters:

Using or sharing Official Sensitive information inappropriately—especially via AI tools—can lead to:

a) Data breaches
b) Legal violations
c) Operational risks
d) Disciplinary action

Reminder:

Always check the classification label on documents or data before using AI tools. If you're unsure whether something is Official Sensitive, consult your line manager or the Information Security Team.

"AI is to be used as digital assistant only – not a Staff Member or Police Officer – and must not be treated, relied upon, or inherit responsibilities as one."

Attempts to use AI for deceptive, harmful, or illegal purposes will result in disciplinary action.

Note: Web-based AI platforms are extremely dangerous due to their ability to retain the information provided by the user within a prompt. This data is stored and used the train the AI Algorithms.

[redacted]

5. Content Evaluation and Accuracy

Users are accountable for the content generated through AI technologies. While AI systems can support efficiency and insight, they may also produce inaccurate, incomplete, or misleading outputs. It is the responsibility of each user to critically assess and verify the reliability, accuracy, and appropriateness of any AI-generated content prior to its use or dissemination.

6. AI Agent Governance

6.1. Agent Types and Approval Process

There are two types of AI Agents:

User-Level Agents

User-Level Agents are AI tools used by staff to support personal workflows and team productivity. These agents may be used for non-sensitive tasks such as summarising documents, generating templates, or improving internal communications.

- Staff may use approved personal agents to work on their own files and team-level content.
- These agents must not access organisational systems or sensitive data.
- Use of organisational data is restricted to force-approved AI agents managed by ICT, SRS, or DSD.
- If a personal agent is proposed to interact with wider systems or sensitive data, it must be submitted to the AI and Automation Standards & Ethics Forum for review and approval.

Admin-Level (Global) Agents

These agents operate across organisational systems or access sensitive data. Only designated administrators within ICT, SRS, or DSD may create or modify these agents.

Proposals must undergo ethical, legal, and technical review, and be approved by both CAB and the Strategic Information Board (SIB) where applicable.

A register of approved AI agents and their intended purposes will be maintained to ensure transparency and accountability.

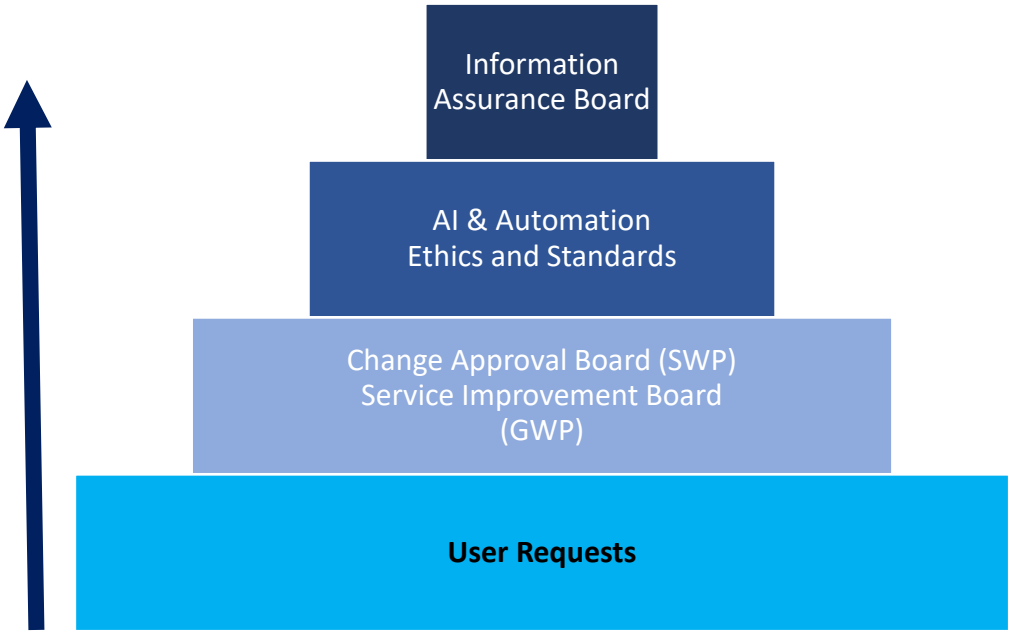
6.2. Role-Based Access Control (RBAC)

RBAC is a key part of AI governance, ensuring that only authorised users can access or manage AI agents. Currently, RBAC is only enforced within LEDS systems used by South Wales Police and Gwent Police. This policy outlines RBAC as an aspirational standard for all AI systems. Broader RBAC enforcement is planned as part of future development and compliance improvements.

Until full implementation, RBAC references in this policy reflect the intended direction, not current operational capability.

6.3. Approval Process

Organisation wide AI Agents or Software Governance Stages:



7. Legislative Compliance

All AI technologies must comply with relevant legislation including but not limited to:

- Data Protection Act 2018
- UK General Data Protection Regulation
- The Human Rights Act 1998
- The Equality Act 2010

COPIES AVAILABLE IN WELSH. CONTACT POLICY UNIT: PolicyUnit@south-wales.police.uk

- Intellectual Property Act 2014
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Investigatory Powers Act (2016)
- Protection of Freedoms Act (2012)
- Public Sector Equality Duty (Equality Act 2010)
- Freedom of Information Act (2000)
- ICO Guidance on AI and Data Protection
- NPCC AI in Policing Covenant 2024
- NPCC AI Playbook for Policing (2025)
- UK Government AI Playbook (2025)
- Parliamentary Briefing on AI Policy Implications (2024)

Regulatory Guidance

- Information Commissioner's Office Guidance and AI and data protection

8. Third-Party References

AI-generated content may occasionally reference third-party products, services, or organisations. Such references must not be interpreted as an endorsement, partnership, or affiliation by South Wales Police and/or Heddlu Gwent Police and/or Heddlu Gwent Police. Users are responsible for ensuring that any such content is appropriately reviewed and, where necessary, amended to avoid misrepresentation or unintended implications.

9. Third Party AI Procurement

All third-party AI technologies must be procured in line with the force Third Party Supplier Assurance policies and procedures.

9.1. Data Protection Impact Assessment

A Data Protection Impact Assessment must be undertaken as part of the consultation process.

9.2. Basic Considerations

Considerations prior to seeking approvals include:

- Police Data must be processed or stored in the UK unless an International Data Transfer Risk Assessment is approved via the DPO and FISO
- Input, processed, stored data must not be shared with other third parties unless specific DPO and FISO approval is provided.

- The third-party supplier must obtain the following accreditations and evidence maintenance of them for the duration of the contract relationship:
    a) ISO/IEC 27001:2022 - Information Security
    b) IASME Cyber Essential & Cyber Essentials Plus (Montpellier) or,
    c) SOC2
- It is desirable that Third-Party Supplier's also evidence compliance or alignment to the following:
    d) ISO/IEC 42001 – Artificial Intelligence Management Systems
    e) ISO/IEC 22301:2019 - Business Continuity Management Systems

10. Training and Awareness

Access to AI tools is conditional upon completion of relevant training. Ongoing awareness campaigns will inform users of emerging risks, updates, and best practices.

11. Enforcement

Non-compliance with this policy may result in disciplinary action, revocation of access, and referral to Professional Standards. All AI use is subject to monitoring and audit.

12. Governance of AI Technologies

AI technologies used within South Wales Police and/or Heddlu Gwent Police must be governed through structured oversight to ensure ethical, legal, and operational compliance. Governance responsibilities are distributed across designated roles and forums to maintain transparency, accountability, and strategic alignment.

12.1. Governance Bodies

To make sure AI is used safely and responsibly, certain types of AI use must be reviewed before they're approved. You should submit a request to the forum if you are:

- Introducing a New AI Tool
- Any new software, app, or system that uses artificial intelligence.
- Using a System That Includes AI Features
- Even if the system isn't fully AI-based, if it has AI functions (like automation, predictions, or decision-making), it needs to be reviewed.
- Making a Major Change to How AI Is Used, for example, using AI in a new way, or applying it to different types of data or tasks.
- Using AI with Personal Information
- If the AI will handle data that can identify individuals (like names, addresses, or case details), it must be reviewed to ensure privacy and legal compliance.

Responsible areas:

a) AI and Automation Standards & Ethics Forum: Reviews all AI proposals for ethical, legal, and operational implications.
b) Information Assurance Board: Oversees information risk and security compliance.
c) ICT and DSD Change Advisory Board (CAB), SIB (Gwent): Manages technical feasibility and release control.
d) Information Governance and Information Security: Conducts DPIAs, risk assessments, and ensures policy compliance.

12.2. Approval Process

All AI technologies must follow a formal approval process prior to deployment:

1) Submit business justification to the AI and Automation Standards & Ethics Forum.
2) Complete DPIA and Information Security Assessment.
3) Consult stakeholders and document concerns.
4) Obtain final approval via CAB or SIB for Gwent.

12.3. Compliance Monitoring

Regular audits and monitoring will be conducted to ensure adherence to this policy. Non-compliance will be escalated to Professional Standards and may result in disciplinary action.

13. Review

This policy will be subject to a minimum of an annual review cycle, in addition to ad-hoc reviews where opportunities for improvement are identified, to ensure its relevance and alignment with the latest industry standards, technological advancements, and regulatory requirements. All revised publications shall be communicated to all users to ensure continuous compliance. It is the user's responsibility to read and abide the contents of each publication.

14. AI Governance & Security Glossary

AI Governance	Framework of policies, procedures, and controls to ensure responsible development, deployment, and oversight of AI systems.
Accountability	The obligation of individuals or entities to report, explain, and be answerable for resulting consequences.
Assurance	Confidence provided by a third party that a system meets its security requirements.

Audit Trail	A chronological record of system activities that enables the reconstruction and examination of the sequence of events.
CAB (Change Approval Boards)	A technical change approval board used to review and approve the technical changes required.
Cyber Essentials Plus	A UK government-backed certification that demonstrates an organisation's commitment to cyber security, including hands-on technical verification.
Data Governance	Management of data availability, usability, integrity, and security in enterprise systems.
Data Minimisation	The principle of collecting only the data necessary for a specific purpose.
Explainability	The degree to which an AI system's internal mechanics can be understood by humans.
IEC/ISO 27001:2022	International standard for information security management systems (ISMS), providing a systematic approach to managing sensitive information.
Information Security	Protection of information from unauthorised access, disclosure, alteration, and destruction.
NIST 2.0	Updated version of the NIST Cybersecurity Framework, providing guidance for managing and reducing cybersecurity risk.
Physical Security	Measures designed to protect personnel, hardware, software, networks, and data from physical actions and events.
Risk Management	The process of identifying, assessing, and controlling threats to an organisation's assets.
Service Improvement Board (SIB)	A governance body focused on identifying, prioritising, and overseeing initiatives to improve services and operational performance.
Transparency	Openness in communication and decision-making processes, especially regarding AI system design and use.
Zero Trust	A security model that assumes no implicit trust and requires continuous verification of user and device identity.

FURTHER INFORMATION AND FORMS

FORMS

LEGISLATION AND REGULATION

FURTHER INFORMATION AND LINKS

AI Toolkit

Joint Supplier Security Questionnaire

DPIA Template

RELATED POLICIES, PROCEDURES AND SOPS

InfoSec Policies

Overarching Data Protection Policy

Joint Information Management Policy

Internal Privacy Policy

CONTACTS

ABOUT POLICY
KEY POINTS
ROLES
FULL POLICY
FURTHER INFO & FORMS
RISKS AND IMPACT
AUDIT
FAQS

RISKS AND IMPACTS

EQUALITY IMPACT

Artificial Intelligence: Acceptable Use - EIA

DATA PROTECTION

N/A

RISK ASSESSMENTS

N/A

AUDIT

DATE	VERSION	KEY CHANGES & COMMENTS	FULL REVIEW?	AMENDMENT BY	AUTHORISED BY
	0.1	New: First Draft	N/A	[redacted]	N/A
	0.2	Re-ordered sections to flow through cycle. Added in roles and responsibilities Table of guiding principles etc Alignment to DPA18	N/A	[redacted]	0.2 Pending Approval
	0.3	Annual review. Adding reference to the use of approved AI Technologies, ICT/DSD Agent management, Change Control, AI / Automation Standards & Ethics Forum	N/A	[redacted]	N/A
	0.4	Removal of references to AI technologies. Official Sensitive examples.	N/A	[redacted]	N/A
	0.5	Gwent comments considered and amended.	N/A	[redacted]	N/A
	0.6	Add AI Agent Governance Model Visual.	N/A	[redacted]	N/A
29/01/26	01	First Published	N/A	[redacted]	[redacted]
	02				
	03				
	04				

	05				
	06				
	07				
	08				
	09				
	10				

FAQS