

PBNI Artificial Intelligence (AI) Policy and Procedures

Policy Owner	
Owner:	Head of Communications
Author:	Information & Governance Officer
Screening and Proofing	
Equality screened:	4 March 2026. Screening completed. No adverse impact identified.
Human Rights screened:	24 March 2026. Screening completed. No adverse impact identified.
Data Protection screened:	1 March 2026. Screening Questions Completed. Although the data protection screening indicated that a DPIA was not strictly necessary, a full DPIA was carried out as a matter of best practice and in accordance with ICO guidance.
Trauma Informed screened:	25 February 2026. Screening was completed, and the policy was updated to incorporate the recommended changes identified in the screening tool
Consultation	
	Internal and external consultation took place between 12 March -10 July 2026.
Approval	
SLT:	17 August 2026
Committee (if required):	PPC 10 September 2026
Board (if required):	17 September 2026
Version	
Version:/Revision Number	100
Publication date:	17 September 2026
Implementation date:	17 September 2026
Review date:	17 March 2027

Document uncontrolled when printed

Document Control

Revision No.	Date	Description
0.1	27 Feb 2026	AIWG – Additional changes made to reflect the opinions of the AIWG members, including the Unions.
0.2	14 April 2026	SLT changes
0.3	21 July 2026	Consultation changes
0.4	11 August 2026	SLT – changes made to reflect stronger narrative around the importance of human oversight and professional practice
0.5	10 September 2026	PPC has approved the Policy and recommended its progression to the Board for approval.
	17 September 2026	Board approved this policy.

Alternative Formats The Probation Board is committed to making its information accessible to all. This document can be provided, upon request, in alternative formats such as large print, Braille, audio, electronic versions, or translated into other languages. Requests for alternative formats should be directed to the Probation Board using the contact details below:

Probation Board for Northern Ireland

80-90 North Street

Belfast

BT1 1LD

Telephone: 028 9052 2522

Email: human.resources@probation-ni.gov.uk

Contents

1.	Rationale.....	4
2.	Aim.....	4
3.	Purpose and Scope	5
4.	Copilot Chat (included at no extra cost in PBNI Microsoft subscription) and Microsoft 365 Copilot licence (extra cost)	6
5.	Authorised Use of AI - Microsoft Copilot	7
6.	Prohibited Uses.....	8
7.	Copilot Use that requires approval.....	9
8.	Resources.....	9
9.	Monitoring and Evaluation.....	10
10.	Policy Review.....	10
11.	Non-compliance	10
12.	AI Procedures	10
13.	PBNI's 8 principles for Responsible use of AI	11
13.1	Human Oversight:	11
13.2	Accountability & Redress:	12
13.3.	Data Governance:.....	14
13.4.	Technical Safety & Security:	16
13.5.	Fairness & Transparency:.....	17
13.6.	Sustainability:.....	17
13.7.	Societal Benefits:	17
13.8	Training and Literacy.....	18
14.	Authorisation Process	18
15.	AI Incident Reporting and Accountability	19
16.	Dissemination and Implementation	19
17.	APPENDIX A – Associated Documents & Policies	21
18.	APPENDIX B - “Prohibited” and “Uses that require approval”.....	23
19.	APPENDIX C – Glossary	24
20.	APPENDIX D – Explanation of Terms	24
21.	APPENDIX E – Legislation	28

1. Rationale

- 1.1. The Probation Board for Northern Ireland (PBNI) recognises the potential of Artificial Intelligence (AI) to support staff, improve efficiency, enhance service delivery, and maximise the value of information and data. AI is identified as a key enabler within PBNI's three-year Corporate Plan, and PBNI commits to exploring opportunities to utilise emerging technologies, including AI, to support the organisation's work. At the same time, PBNI is committed to ensuring that any adoption and use of AI is safe, lawful, transparent, and aligned with public service values and organisational policies.
- 1.2 In respect of probation professional practice AI use, at this juncture, will be primarily used for administrative, corporate, information management, communications and business support activities. AI must not replace professional probation judgement, relationship-based practice, direct engagement with service users, victims or partner agencies, or any assessment, recommendation or decision requiring professional expertise. Responsibility and accountability for all professional opinions remain with the relevant member of staff and cannot be delegated to an AI system.

2. Aim

- 2.1. AI should be regarded as a key component of public service transformation, but it must be placed within a strong governance framework, with strong ethics, a commitment to open communication and full transparency, in order to maximise trust and mitigate risks. PBNI recognises that effective probation practice relies upon professional relationships, communication and professional judgement. AI cannot replace direct engagement between probation staff and service users, victims, families, communities or partner agencies. This policy aims to provide the governance framework for the ethical, secure, responsible and legal use of artificial intelligence.

3. Purpose and Scope

- 3.1.** This policy outlines the principles for the responsible use of Artificial Intelligence (AI) within PBNI. It applies to all employees, Board members and students. The main AI tool currently available for use by staff in PBNI is Microsoft Copilot Chat (included at no extra cost in PBNI Microsoft subscription) and Microsoft 365 Copilot licence (extra cost).
- 3.2.** PBNI encourages the responsible use of AI to provide more efficient, innovative and cost-effective services. However, because the use of “AI Tools” as defined in this Policy raises a variety of legal and compliance concerns, it is crucial when an AI Tool is being used, it is done so in a manner consistent with this Policy and all other applicable PBNI Policies and Procedures. [\(Appendix A\)](#) Certain uses may require approval and/or a licence as set out in the [AI Use – Approval Proforma](#).
- 3.3.** Within the scope of this policy, AI refers to any machine-based system that can automatically generate predictions, content, recommendations or decisions using any of the following techniques.

(i) Logic and knowledge-based systems of AI encode knowledge and solve problems using logical statements and rules. Example applications include proving mathematical theorems, fault diagnosis and playing chess.

(ii) Machine Learning systems learn and improve from examples without all its instructions being explicitly programmed and can extrapolate knowledge to unfamiliar situations. Examples of this include all computer vision, pattern detection, Large Language Models (LLM) and Generative AI.

(iii) Optimisation and Statistical Techniques include predictive statistics, time series analysis, and probability theory. However, simple descriptive statistics that summarise data without making predictions are not

considered AI (unless they also come under category i or ii above) and are excluded from this policy.

(iv) Any software system that does not leverage any of the above techniques and is not used to automate or recommend a decision, classify data, or predict an outcome is generally not considered AI and is therefore not covered by this policy. This is not exhaustive as the field of AI is fast changing at the time of writing.

(v) Microsoft 365 Copilot which is the main AI tool available to staff is a generative AI assistant powered by large language models (LLMs) and the differences between the licenced and unlicensed version are explained below.

4. Copilot Chat (included at no extra cost in PBNI Microsoft subscription) and Microsoft 365 Copilot licence (extra cost)

4.1 All staff members in PBNI have access to Copilot Chat through their standard Microsoft 365 subscription. Microsoft 365 Copilot licence can be requested; however, staff must complete the 'AI Use and Licence Approval Proforma' providing a clear rationale for requiring the licenced version. The staff member will also need to ensure they have consulted with the budget holder and obtained confirmation that sufficient resources are available to cover the cost of the licence.

4.2 What are the differences in Copilot Chat and Microsoft 365 Copilot?

Copilot Chat (web) (signed in to our account and displaying the protected shield) does not have access to Sharepoint, OneDrive, Exchange or Teams content. It is web-grounded and can only access information, uploaded or pasted into the tool by the user.

Microsoft 365 Copilot licence works inside users' M365 content, such as emails or spreadsheets. It can summarise meetings and e-mail threads. It will also apply the same permissions, sensitivity labels and retention to existing records.

For further information on the difference between the tools please see [Record PB1/26/0010887: Microsoft copilot chat and Microsoft 365 Copilot Compliance](#)

- 4.3 In respect of Copilot Chat no sensitive information, special category data or criminal offence data should be entered into it. Only very minimal personal data can be entered into Copilot Chat for example the names of attendees at meetings. In respect of Microsoft 365 Copilot, it may process information already held within authorised Microsoft 365 systems subject to existing permissions and controls.

5. Authorised Use of AI - Microsoft Copilot

- 5.1. There are scenarios where Microsoft Copilot Chat can and is encouraged to be used in the course of daily tasks without prior approval. This involves inputting any non-sensitive information to the Microsoft Copilot Chat that would be available on the PBNI website or which PBNI would disclose to the public if requested. Some examples of where staff can use Copilot to assist in administrative tasks are:

- ✓ Drafting responses to general enquiries.
- ✓ Summarising documents or policies.
- ✓ Creating presentations.
- ✓ Drafting lines for media or publications.
- ✓ Drafting documents that will be publicly available.
- ✓ Drafting AQ responses.

- ✓ Drafting internal reports, letters, or emails which contain no special category data or criminal offence data and very limited personal data such as names of senior members of staff or names already available on PBNI website.
- ✓ Drafting external letters which contain no special category data or criminal offence data and very limited personal data such as names of senior members of staff or names already available on PBNI website.
- ✓ Providing graphics for social media, posters, leaflets.
- ✓ Drafting agenda and assisting with minutes for meetings which contain no special category data or criminal offence data and very limited personal data such as attendees at meetings.

5.2. In all the above scenarios staff should not input to Microsoft 365 Copilot Chat sensitive data and the most limited personal data. If in doubt about when Microsoft 365 Copilot Chat can be used staff should seek advice from the Information Asset Owner, Information Governance Officer or Data Protection Officer.

6. Prohibited Uses

6.1. If the proposed use of an AI Tool is prohibited by PBNI, it may not be engaged in under any circumstances.

6.2. Prohibited Uses: Refer to [Appendix B](#) for a list of examples where Copilot or any other AI tool cannot be used. Such prohibited uses are generally those that create an unacceptably high risk to the fundamental rights of individuals, or which present an unjustifiable risk to PBNI. AI must not be used to analyse service user behaviour, assess likelihood of reoffending, determine intervention needs, or make decisions / recommendations relating to breach, recall or release.

6.3 Where staff have use of AI products (especially generative AI) on their own devices (i.e. personal devices not managed by PBNI) they should be aware that these should not be used for work purposes. Examples of these types of AI

products include chat (ChatGPT), copywriting (Copy.AI, Notion.ai), and many more, including tools that have AI functionality embedded in them. If there is a need to use any other form of AI for work purposes such as ChatGPT a separate DPIA should be considered and the [AI Use – Approval Proforma](#) must be completed and approved.

7. Copilot Use that requires approval

- 7.1.** Where a member of staff wants to use Microsoft Copilot Chat outside of the authorised use scenarios set out in section 5, approval is required from the IAO (Information Asset Owner), and the AIWG (Artificial Intelligence Working Group) must then recommend approval to the Senior Information Risk Owner (SIRO) Where uncertainty exists regarding whether a proposed activity is prohibited, staff should seek advice before proceeding. Early discussion is encouraged to support safe innovation and learning. Likewise, if staff have researched and found that another AI tool could be of assistance to their work, approval is required via the IAO, AIWG and SIRO using the proforma.
- 7.2.** Refer to [Appendix B](#) For a list of examples of uses which require approval. In such cases, use may be permitted but will first require completion of [AI Use - Approval Proforma](#). These uses will be subject to the recommendation of the IAO, and final approval by the SIRO.
- 7.3.** Approval decisions will consider data protection risk, operational benefit, technical safety, and budgetary requirements.
- 7.4.** Where approval is not granted, feedback can be provided.

8. Resources

- 8.1.** There is a resourcing need to ensure there is sufficient staff to maintain and oversee the AI approval process and provide the governance framework and

human oversight functions required to oversee the implementation and monitoring of AI.

- 8.2.** There is a resource requirement for Copilot licences should they be approved for use.

9. Monitoring and Evaluation

- 9.1.** AI is fast changing and developments are ongoing. This means that this policy will be kept under review to ensure it is in keeping with current legislation and good practice.

10. Policy Review

- 10.1.** PBNI's policies are reviewed every 4 years, unless there are legislative or regulatory changes that will affect the policy. The use and laws on AI are evolving at an accelerated rate; therefore, this Policy will be reviewed in 6 months, 12 months, 18 months and 2 years and every year thereafter. Any updates will be communicated to all relevant stakeholders in a timely manner.
- 10.2.** Staff feedback can be submitted through the Information Governance Officer.

11. Non-compliance

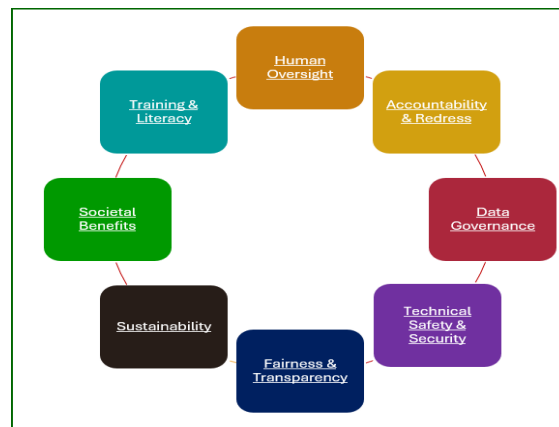
- 11.1.** All staff are responsible for the implementation of this policy and procedures and should ensure that they read and understand it. PBNI will prioritise learning and improvement alongside compliance. Non-compliance of this policy may however result in disciplinary action as outlined in PBNI's Disciplinary Policy.

12. AI Procedures

Please see procedures below.

13. PBNI's 8 principles for Responsible use of AI

PBNI have set out 8 principles for responsible use of AI. These principles are adopted from Northern Ireland's AI Strategy (currently being consulted on) and are designed to build public confidence and trust. All PBNI staff using AI must adhere to these 8 principles.



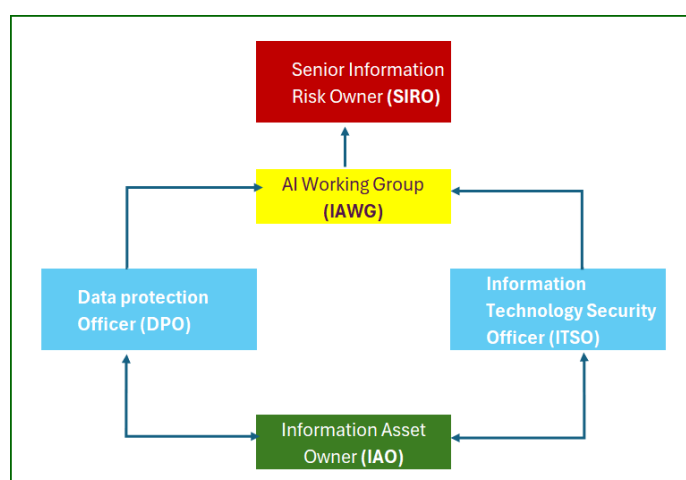
13.1 Human Oversight:

Human Oversight is the critical practice of PBNI staff using professional judgement to ensure safety, minimising bias, preventing hallucinations and maintaining accountability. Human oversight extends beyond simply checking factual accuracy; staff must critically evaluate outputs using professional knowledge and understanding. AI outputs must never be accepted solely because they appear well written. As all AI Tools may be prone to inaccuracies, hallucinations, omissions, biases, and other misleading or undesired results, their output must always be verified for accuracy and completeness by using independent and trustworthy sources, as with any other work product. Staff may use a verification prompt such as 'before responding, check your sources to ensure the information is up-to-date and include citations for all claims' or an accuracy check prompt such as 'I need to check the accuracy of this information, please compare this against reliable sources', it is important staff review all output.

13.2 Accountability & Redress:

Accountability - Clear lines of responsibility are critical for the successful use of Copilot. This clarity is essential for auditing purposes, but it is also valuable in ensuring the decision-making process is explicit. The diagram below shows the authorisation process for using AI outside of the agreed purposes in section 5 and obtaining a Microsoft Copilot licence within PBNI.

Figure 1 – Ownership and accountability organisational chart



Information Asset Owner

Each Information Asset Owner (IAO) within PBNI holds a pivotal role in ensuring that they and all colleagues within their line management remit, fully understand and adhere strictly to this Policy. Their role is to understand what information is held in their business area, what is added, what is removed, how information is moved, who has access and why. They should also understand and address risks to the information's confidentiality, integrity and availability, ensure it is managed in compliance with the law and be a source of assurance to the SIRO. IAOs need to manage information assets to comply with statutory obligations (such as Freedom of Information Act, the Data Protection Act). The Information Asset Owner must also ensure that the use of AI in their business area is recorded on the AI Impact, Risk and Governance database via the Information Governance Officer.

AI Working Group (AIWG)

A dedicated working group has been established and is tasked with providing oversight of AI use in PBNI. The role of this group is to consider and make recommendations as to what areas of business in PBNI MS Copilot could and/or should be used for, taking account of practice in the wider public sector, both in NI and further afield. It also establishes through the development of policies and procedures a clear decision-making process and governance arrangements about the use of AI. It is also responsible for scoping out training for staff in the use of MS Copilot.

Senior Information Risk Owner

The SIRO, who is the Chief Executive holds overarching responsibility for governance and the proactive management of information-related risk associated with AI technologies. It is the SIRO's duty to ensure the robust frameworks, comprehensive risk management processes, policies and controls are effectively implemented and maintained throughout PBNI. The SIRO has the final approval for the use of AI in PBNI. They will provide assurance to the Board and its committees that AI in PBNI is being used within the policy framework and legislative requirements.

Data Protection Officer

The Data Protection Officer is responsible for ensuring that the use of AI meets data protection, privacy and information security requirements, in accordance with the UK GDPR and Data Protection Act 2018. They will provide advice and guidance to staff on compliance with data protection and records policies in respect of the use of AI.

Information Technology Security Officer (ITSO)

The ITSO is responsible for giving technical advice and guidance to ensure the safe and secure use of AI Tools and Systems within PBNI in liaison with our

Network & Infrastructure provider and Cyber Security colleagues in Digital, Security & Finance Shared Services, DoF.

Information & Governance Officer

The Information & Governance Officer will be responsible for the development and review of governance policy and procedures regarding use of AI Tools and Systems in PBNI. They will be responsible for coordinating ideas about how PBNI can use AI innovatively in a way that promotes efficiency and effectiveness.

Redress

Individuals who wish to raise concerns about the use of AI and their data protection should email the Data Protection Officer mailbox: DPO@probation-ni.gov.uk.

13.3. Data Governance:

PBNI will ensure that any data used is subject to the highest standard of data governance. Therefore, PBNI will adhere to data protection legislation including the Data Protection Act 2018, UK GDPR, and the Computer Misuse Act 1990 and the 7 data principles in the use of Generative AI. As with any other processing of personal data, Generative AI developments must take the approach of data protection by [design and by default](#).¹ This means at the earliest stage when considering use of AI staff must consider any related privacy risks and mitigate them.

A Data Protection Impact Assessment (DPIA) screening should be considered by the IAO for uses of AI within their business area outside of those authorised

¹ [Data protection by design and by default | ICO](#)

for use in this policy. The Data Protection Officer can provide advice and guidance on completion of DPIA screenings. The DPIA should include:

- A systematic description of the processing activity, including data flows and the stages when AI processes and automated decisions may produce effects on individuals;
- An explanation of any relevant variation or margins of error in the performance of the system which may affect the fairness of the personal data processing and;
- A description of the scope and context of the processing, including:
 - What data you will process.
 - The number of data subjects involved.
 - The source of the data.
 - To what extent individuals are likely to expect the processing.

Your DPIA should identify and record the degree of any human involvement in the decision-making process and at what stage this takes place.

There is a need to be exceptionally careful around the use of personal data and only the most limited personal data should be entered into Copilot Chat. Personal data such as names, addresses and of service users, victims, employment candidate should not be entered. Only minimal personal data of PBNi staff such as attendees at meetings are permitted to be entered into Copilot Chat.

Special category or sensitive data must not be used in the process of using AI. Special category or sensitive data is defined as: data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data or data concerning sex life or sexual orientation. Criminal offence data must not be entered into AI.

AI systems may occasionally generate inaccurate and misleading information. The Information & Governance Officer in PBNI will monitor such occurrences through user feedback. Any confirmed hallucinations must be logged by the Information & Governance Officer and used for training purposes. Lessons learned will be shared across teams to strengthen safe use and reinforce the requirements for human verification of AI

13.4. Technical Safety & Security:

Microsoft Copilot Chat is available to all PBNI Users and Microsoft Copilot (licenced version) is currently available to a small number of staff who have been granted approval for a specific reason. PBNI staff must seek approval to use other AI tools such as Chat GPT on their work devices for PBNI work purposes.

PBNI has no oversight over how data, which is entered into web-based Generative AI model, is subsequently used by others. Therefore, you should not put information into Generative AI models that, if compromised or lost, could have damaging consequences for individuals, service users or for PBNI more generally.

The security concerns about the use of AI can include;

- It can get things wrong and present incorrect statements as facts (a flaw known as 'AI hallucination').
- It can be biased and is often gullible when responding to leading questions.
- It can be coaxed into creating toxic content and is prone to 'prompt injection attacks'.
- It can be corrupted by manipulating the data used to train the model (a technique known as 'data poisoning').

Staff uncertain about technical risks should seek advice from IT or governance colleagues before proceeding.

13.5. Fairness & Transparency:

The use of AI Tools and systems must be fair and transparent. If an AI tool is used to influence a decision the rationale must be explainable and the PBNI record must clearly display that AI has been used in its development.

PBNI's privacy statements will contain information for service users, partners and staff about how AI is used in PBNI. Staff must clearly acknowledge when AI tools have been used to support the drafting, analysis and development of externally published reports and documents for example PBNI Annual Report, Equality Reports or Statistical reports. Staff should confirm that all outputs have been reviewed and validated. PBNI will have a statement on its website to say generative AI may be used on some occasions to assist in the drafting of materials.

An example foot note should state "An AI tool was used to support the drafting of this document. The final content has been checked and approved by the author, who is responsible for its accuracy"

All uses of AI in PBNI should uphold values of fairness and inclusivity without discrimination or bias against any demographic or individual. It is critical that bias detection or ethical concerns identified during AI Usage must be explicitly documented, addressed and mitigated.

13.6. Sustainability:

The NI Executive's Climate Action Plan has an overall target to achieve net-zero greenhouse gas emissions by 2050 with annual carbon budget targets also agreed. Therefore, the authorisation of use and approach to AI use must consider energy sources and efficiencies across all the stages of the AI lifecycle.

13.7. Societal Benefits:

When considering future AI use, PBNI must consider how the usage will enhance efficiency and drive innovation to improve its service delivery to communities.

13.8 Training and Literacy

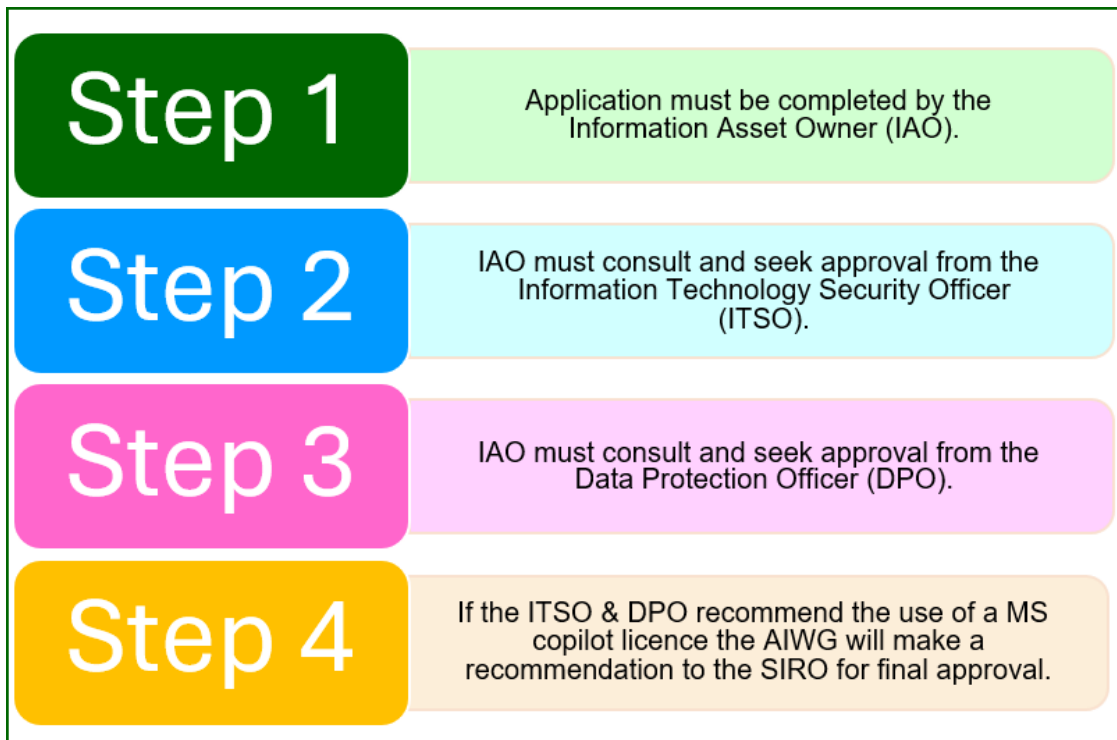
In the longer-term AI will drive demand for new technical skills and also bring wider changes to the overall skills landscape, thereby requiring a particular focus on the evolution of all levels of education and training within PBNI. In the shorter term PBNI will ensure that all staff have access to appropriate training to support the safe and responsible use of Microsoft Copilot.

14. Authorisation Process

14.1. PBNI is committed to identifying and capturing opportunities arising from emerging technologies. Business areas can research and find out more about Microsoft Copilot, expand their understanding of how they can be used, how they work, and ensure they are used in a safe and ethical manner.

14.2. PBNI has developed the following authorisation process for the use of AI outside those specified in this policy and the application of Copilot licences within PBNI. Staff wishing to use AI for a new or different purpose outside of those outlined in Section 5 must complete the authorisation process.

14.3. AI Use & licence Approval Proforma



15. AI Incident Reporting and Accountability

As is the case with any data protection incident if whilst using AI a data incident or breach occurs the data incident procedures must be followed. [Data Incident Response Procedures 2022 - 2026](#)

16. Dissemination and Implementation

This policy will be disseminated through a structured internal communications plan ensuring that all colleagues are informed of its purpose scope and application. Communication will include targeted briefings to teams alongside organisational wide updates via established internal channels such as the Probation News and Town hall and Quarterly Area Manager's meetings.

This policy will be saved in the designated policy section within Content Manager and also be published on PBNI's intranet, ensuring ease of access for all staff. Where future reviews or amendments have been made to the policy these changes will be communicated clearly and properly through appropriate channels including Probation News, Area Manager meetings or direct communications via the Head of Communications.

17. APPENDIX A – Associated Documents & Policies

Name of Document	Record Number	CM. Link
AI Use and Licence Approval Proforma	PB1/26/0036213	AI Use and Licence Approval Proforma
Artificial Intelligence Impact Accountability and redress Assessment Database	PB1/26/004053	AI Bias Monitoring and Redress Log
Copilot Chat User Guidance	PB1/25/0040327	Copilot Chat User Guidance – August 2025
Artificial Intelligence – Guidance for All PBNI Staff – Gail McGreevy August 2025	PB1/26/0004057	Artificial Intelligence- Guidance for PBNI Staff – Gail McGreevy August 2025
Data Protection Policy	PB1/22/0007019	POLICY – Data Protection Policy (2022)
Freedom of Information Policy	PB1/25/0028628	Freedom-of-Information-Policy and Procedure - 2026
Data protection Privacy Impact Assessment template (DPIA)	PB1/22/0007552	Data Protection Privacy impact assessment - AI Policy 2026
Disciplinary Policy		Disciplinary Policy and procedures - 2025

ICO Guidance on use of AI		Guidance on AI and data protection ICO
UK Gov Generative AI Framework		https://www.gov.uk/government/publications/generative-ai-framework-for-hmg/generative-ai-framework-for-hmg-html
NCSC Guidance		https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development/guidelines/secure-development
NICS Use of Generative Artificial Intelligence (AI)		http://nics.intranet.nigov.net/nics/documents/nics-use-generative-artificial-intelligence-ai
ICO – Data Protection by design and by Default		Data protection by design and by default ICO
Data Incident Response Procedures 2022-2026		Record PB1/23/0065612: PROCEDURES - Data Incident Response Procedures 2022 - 2026

18. APPENDIX B - “Prohibited” and “Uses that require approval”

Appendix B provides examples of where the use of AI is strictly prohibited and examples of those areas that require prior approval. Both lists are not exhaustive.

PBNI recognises the technical and use-specific details concerning an AI Tool may not clearly fit within any defined category.

Examples where the use of AI is prohibited:

- AI must not be used to analyse service user behaviour, assess likelihood of reoffending, determine intervention needs, or make decisions / recommendations relating to breach, recall or release.
- Writing Magistrate Court Reports, Pre-Sentence Reports, Reports for the Parole Commissioners, Designated Risk Manager Reports.
- Entering any personal details of a service user, or victim.
- Assessing or predicting a person’s risk of criminality/offending or recidivism. AI must not be used to assess, predict, score or recommend decisions relating to risk of harm, likelihood of reoffending, vulnerability, suitability for interventions, case planning, public protection measures, enforcement action, breach, recall or suitability for release.
- Generating or manipulating images, audio or video content that appreciably resembles or replicates existing persons, places or events and would falsely appear to a person to be authentic (a “deep fake”) without clear disclosure that the content has been artificially generated or manipulated.
- Anything that is illegal.
- Making decisions based upon, categorising, or discriminating against people based on their race, colour, age, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation, sex, gender, gender identity, disability, or genetic information or other legally protected characteristic.

Examples where use of AI would need approval:

- Request for a licenced version of Copilot.
- Request to use Copilot for any new project in PBNI.
- Request to use ChatGPT or any other AI tool for work purposes.

19. APPENDIX C – Glossary

IAO	Information Asset Owner
DPO	Data Protection Officer
SIRO	Senior Information Risk Owner
AI	Artificial Intelligence
ITSO	Information Technology Security Officer
PBNI	Probation Board for Northern Ireland

20. APPENDIX D – Explanation of Terms

Artificial Intelligence (AI)	AI refers to computer systems capable of performing tasks that historically required human intelligence such as speech recognition decision making and pattern identification AI is an umbrella term that encompasses various technologies such as machine learning, deep learning and natural language processing (NLP). When people use the term AI today they often refer to machine learning powered technologies like chat bots computer vision and other systems that enable
------------------------------	--

	machines to perform tasks previously exclusive to humans
Generative Artificial Intelligence (GenAI)	GenAI also known as generative AI or GAI is a subset of AI that can generate new content (such as text, images, videos or other data) in response to prompts. Generative models learn patterns and structure from training data and then generate new data with similar characteristics.
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. DPIAs must be considered and where necessary completed in full for any new data processing activities, new systems, services, and commissioning activities.
Machine Learning (ML)	Machine learning is a field of study within artificial intelligence (AI) that focuses on developing and analysing statistical algorithms. These algorithms learn from data and generalise their knowledge to perform tasks without explicit instructions. In other words ML enables machines to improve their accuracy over time by imitating how humans learn. It finds applications in various domains including natural language processing, computer vision and speech recognition to name a few.
Natural Language Processing	Natural language processing is a branch of computer science or AI that gives computers the ability to understand, interpret and generate human language in both written and spoken forms
Processing	Processing means doing anything with personal data. Under data protection laws processing is a very broad term. It includes any action taken with information about a person, whether done manually or electronically.

AI Hallucinations	An AI hallucination is a phenomenon where an artificial intelligence model generates or perceives patterns, objects or meanings in data that do not actually exist. This has now been observed across various AI models and continues to be prevalent today
AI Bias	In the context of artificial intelligence, AI bias refers to the tendency for an AI system to produce results that are systematically prejudiced due to erroneous assumptions in the machine learning process. This could occur due to various factors including; Biased Data: If the training data used to develop the AI model contains biases the AI system is likely to replicate those biases in its outputs Algorithm Limitations: The design of the AI algorithms themselves can produce biases especially if they are not properly calibrated to handle diverse data. Human Influence: The biases of the developers and data scientists who create and train the AI systems can inadvertently become embedded in the models. These biases may result in unfair or discriminatory outcomes.
Algorithmic Transparency	Algorithmic transparency refers to the ability to understand and explain how an AI system makes decisions.
AI Ethics	AI ethics encompasses the moral implications of AI technologies including fairness, transparency accountability and non-discrimination. Ethical AI

	ensures that AI technologies are designed and implemented in ways that protect human rights promote fairness and avoid harm especially in relation to the information PBNI holds.
AI Lifecycle	The AI lifecycle refers to the stages an AI system goes through from conception to deployment and ongoing monitoring. It includes data collection, model development, training, deployment, performance evaluation, and continuous improvement.
Bias Mitigation	Bias mitigation refers to the processes and techniques used to reduce bias in AI models including strategies such as data pre-processing, algorithm adjustments and post-processing methods that aim to minimise unfairness in AI outcomes.
Automated Decision Making	Automated decision making refers to decisions made by AI systems without human intervention. These decisions are typically based on data inputs on pre-set algorithms. In PBNI automated decision making can assist in the administrative tasks but must be overseen to ensure compliance with legal and ethical standards
Data Governance	Data governance refers to the policies and processes in place to manage the availability, usability, integrity and security of data within PBNI. Effective data governance ensures that data used for AI systems is accurate, secure, and used responsibly in compliance with data protection regulations such as GDPR.
AI Bias/Hazard log	An incident or hazard log is a dynamic document used to record identified hazards associated with AI systems within PBNI. It documents the risks, their potential impact and controls implemented to mitigate these risks. The hazard log is regularly updated as new risks emerge and as part of an ongoing monitoring system

Human-AI Collaboration	Human AI collaboration refers to the interaction between probation staff and AI systems. This includes how AI tools assist staff in decision making while maintaining human oversight and control to ensure compliance AI should support not replace individuals.
------------------------	---

21. APPENDIX E – Legislation

UK General Data Protection Regulation 2016, Data Protection Act 2018,) Data Use and Access) Act 2025	Data protection legislation governs how personal data is processed including by AI systems and provide statutory rights including the right to object to automated processing to challenge and prevent decisions made solely by automated systems that significantly affect them
Human Rights Act 1998	Protects fundamental rights and freedoms including privacy and freedom of expression which may be affected by AI use
Freedom of Information Act (FOIA) 2000 and Environmental Information Regulations 2004	Under the FOIA/EIR, PBNI has a duty to make information available to the public upon request, unless specific exemptions apply it is also obliged to proactively and routinely publish information that has been frequently requested in the past on its website.
Computer Misuse Act 1990	The Computer Misuse Act 1990 (CMA) aims to protect the integrity of computer systems and data by criminalising unauthorised access (hacking), unauthorised modification of data, and

	the creation or supply of tools used for these purposes. It covers AI-enabled crimes through its technology-neutral nature, allowing prosecution when AI is used as a tool for unauthorised access, to create malicious software, or to facilitate fraud. While current laws are applied to AI, the government is reviewing the Act to specifically ensure emerging AI-driven threats.
--	---