HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:16/12/2025

2025/1217 - Artificial Intelligence (AI)

In response to your recent request for information regarding;

I am investigating how AI-assisted evidence analysis is documented and reported within existing Chain of Custody (CoC) and Audit Trail (AT) structures.

For the sake of clarity, I have included a glossary at the end of this document. CoC is used here as an umbrella term encompassing related concepts such as continuity, chain of evidence, and provenance; while AT refers to any documentation system that captures and records the forensic processing of evidence.

List of Questions
1. Does your police force deploy Artificial Intelligence (AI) systems in areas including investigation, intelligence, operations, case management, or evidence processing?

No, but we are considering it

If yes, please provide:

I. The names of the tools, underlying technology, software versions, and primary use cases.
II. Whether each tool is internally developed or procured from third-party providers.
III. The name of the providers and a copy of any related contract documents.
IV. The current status of each tool (in trial/pilot stage, under evaluation, or fully deployed).
V. Whether each AI tool is embedded in any forensic platform(s), or whether it operates as a separate, standalone system for specific tasks.

2. Does your police force use Natural Language Processing (NLP), including Large Language Models (LLMs), Automatic Speech Recognition (ASR), or other AI technologies for processing and analysing forensic audio and textual evidence, (covering tasks including transcription, speaker diarisation, translation, summarisation, redaction, document generation, or form-filling)?

No, but we are considering it

If yes, please provide:

I. The names of the tools, underlying technology, software versions, and primary use cases.
II. Whether each tool is internally developed or procured from third-party providers.
III. The name of the providers and a copy of any related contract documents.

IV. The current status of each tool (in trial/pilot stage, under evaluation, or fully deployed).
V. Whether each AI tool is embedded in any forensic platform(s), or whether it operates as a separate, standalone system for specific tasks.

3. Does your force have any specific policies, or protocols governing the use of AI tools in processing and analysing forensic audio and textual evidence, or other forms of evidence?

Please attach or reference any documents related to this.

Yes, the AI Policy applies to any, and all uses of AI
Please see attached.

4. Is the chain of custody (CoC) and/or audit trail (AT) recorded when digital evidence, broadly speaking, are processed and analysed?

Yes.
North Wales Police (NWP) Digital Forensic Unit (DFU) are accredited and audited by UKAS against the Forensics Science regulators Codes and ISO 17025 standard, this compliance is documented on the UKAS website, the audit that takes place also covers information security.

If yes, please provide:

I. Details of the information that is recorded (e.g., evidence identifiers, date/time of transfers, personnel identifiers, storage/access logs, integrity checks)

DFU uses a case management system when capturing digital evidence at the point in which the data is ingested the captured data is uploaded to a server with auditing logs. The process is documented using standard operating procedures, along with SOPs for the process there are also data management processes and procedures in place.

II. Details of any technical or procedural methods used to record or track the CoC and/or AT. Kindly specify if the process is automated, manual, or hybrid.

I would reference the beginning to end process as hybrid with some elements of manual and some elements of automation. In essence the captured data is uploaded to a server with system logging in place. The systems are only accessible by DFU staff.

III. Please indicate whether any verification or validation procedures are in place to confirm that digital evidence, upon acquisition, is a genuine and unmodified record rather than a synthetically generated or manipulated.

Data is systematically checked from capture, this is a hashing-based verification, the digital forensics tools that are used check the integrity of the data being used, following this DFU staff also verify data when moving storage locations.

IV. Any guidelines, practice directions, or policies guiding the documentation of CoC and/or AT for digital evidence, including any templates or forms. Kindly attach or reference related documents.

There are a number of processed used within DFU. However, concerns have been raised in disclosing the standard operating procedure (SOP) in to the public domain. A Freedom of Information Act request is not a private transaction. Both the request itself, and any information disclosed, are considered suitable for open publication. This is because, under Freedom of Information, any information disclosed is released into the wider public domain, effectively to the world and not just to one individual.

Therefore, Section 31 (1) (a) Law Enforcement is to be considered as part of the Public Interest Test. A Public Interest Test has been carried out to weigh up the reasons for and against disclosure

of the information requested, to ensure the release is in the interest of the public as a whole and not just the applicant.

Section s31(1) Law Enforcement

Section 31 (1) is a prejudice based qualified exemption, therefore there is a requirement to articulate the harm that would be caused in confirming or not that the information is held as well as carrying out a public interest test.
The Harm Test process requires North Wales Police to consider any possible harm that might arise as a result of placing the requested information into the public domain. This process considers the potential harm to:

- Individuals
- The community as a whole
- North Wales Policeand the wider policing service
- Other bodies

Harm in respect of s31(1) Law Enforcement

To disclose particular policing tool of this type used by North Wales Police as part of an investigative process could reveal operational tactics linked to policing, compromise police investigations and/or adversely affect the ability of North Wales Police and others to safeguard.
It is well established that police forces utilise Digital Forensic techniques in order to counteract criminal behaviour, detect crime, and assist in the apprehension and prosecution of offenders. Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. In this case the information relates to a service provider and by extension their products for the extraction of data from devices.
By revealing specific tactical information such as requested within this request, it would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders. When considered on a Force by Force basis, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

Public Interest Test:

Factors favouring Disclosure – Providing details of operating procedures would provide the public with information about technologies and North Wales Police capabilities. This would reinforce the wider commitment to openness and transparency with the general public and facilitate public debate. Furthermore, owing to the inherent link between transparency and public confidence, would likely to improve the general public's confidence. Over time, an increase in public confidence would be likely to improve public engagement with the police. This would, in turn, lead to an improvement in our ability to both prevent and detect crime, and apprehend and prosecute offenders.

Factors favouring Non-Disclosure – Disclosing operating procedures used would provide our capabilities to persons intent on disrupting their work, with information that would assist them to do so. In this case, for the reasons outlined in the evidenced harm, the effectiveness of current and future strategies when carrying out investigations and gathering evidence may be compromised. The safety of the public is of paramount importance to policing purposes, and any increase in crime would place the public at risk of harm. When the current or future law enforcement role of the force may be compromised by the release of information, the effectiveness of the force will be reduced.
The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, disclosing tactical information relating to the extraction of data from computers and other devices, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

Balance Test

Having considered the reasons why North Wales Police should disclose operating procedures, although openness and transparency is at the forefront when considering the public interest, in this case disclosure relating to Digital tools used by the police for investigative purposes would not be in the public interest.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with any information that is released. Disclosing the systems used would reveal specific policing activity in the digital sphere of investigations and would assist those intent on causing harm. This would directly harm the ability of the force to investigate crime. This could also reveal police capabilities, compromise police investigations and/or otherwise. I have attached considerable weight to these interests as the primary role of the Police Service is to both prevent and detect crime and apprehend those responsible for committing criminal offences.
Therefore, at this moment in time, it is our opinion that for these issues the balance test for confirming, nor denying, that information is held is made out.

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

V. Has your force conducted any internal evaluations or comparisons regarding the efficiency, accuracy or reliability of automated, manual, or hybrid reporting methods? If yes, please provide copies or references.

There have been validation studies undertaken which forms part of our ISO accreditation for capture. We are not able to provide copies as per the public interest test above.

VI. Is the maintenance of a CoC and/or AT managed in-house or outsourced?

a. If in-house, provide details of the responsible role(s) or department(s), including any training materials or internal guidance relevant to this task.

The CoC is considered to be the responsibility of all involved in the investigation process within DFU from capture to reporting, the data is forensically captured and hashed the hash is checked at multiple steps along the process, the whole process for training and mentoring is supportive of data integrity. The original data source that is captured is also retained during the investigation.

The AT is managed using server technology the servers are supported by both NWP DFU staff and external IT company whom supports the servers.

b. If outsourced, please provide the name of the provider(s), a description of their role, and any related contract document(s).

N/A

5. Is the chain of custody (CoC) and/or audit trail (AT) recorded when AI systems are used in processing and analysing forensic audio and textual data, or other forms of evidence?

Not used at present, but we are considering it, and if used there would need to be an audit trail for it to comply with the AI policy.

If yes, please provide:

I. Details of the information that is recorded, which may include but is not limited to: identifier of the evidence, details of the AI model (e.g., version, provider), verified error rates, and identification of human oversight (if applicable).

II. Please indicate whether any paradata is captured during the processing of digital evidence. By paradata, I refer to information generated as a by-product of human interaction with the AI systems during evidence processing (e.g. prompts, edit history, data discards, interaction logs, correction logs, reviewer annotations, parameter adjustments, iterations).
III. Details of any technical or procedural methods used to document CoC and/or AT of AI-assisted evidence analysis, including any templates or forms. Kindly specify if the process is automated, manual, or hybrid.
IV. Has your force conducted any internal evaluations or comparisons regarding the efficiency, accuracy, or reliability of automated, manual, or hybrid reporting methods? If yes, please provide copies or references.
V. Any guidelines or practice directions guiding the documentation of CoC and/or AT specific to AI-assisted evidence analysis. Kindly attach or reference related documents.
VI. Is the maintenance of a CoC and/or AT managed in-house or outsourced?
a. If in-house, provide details of the responsible role(s) or department(s), including any training materials or internal guidance relevant to this task.
b. If outsourced, please provide the name of the provider(s), a description of their role, and any related contract document(s).

6. Are human reviewers involved in reviewing, correcting, or contributing to the outputs generated by the AI systems in processing and analysing forensic audio and textual evidence?

Not used at present, but we are considering it, and if used there would need to be an audit trail for it to comply with the AI policy

If yes:

I. What is the formal description of the role(s), and what specific responsibilities do individuals in these roles carry out?
II. What training materials or internal guidance are provided to support these roles?
III. How is human contribution tracked and distinguished?
IV. Are records maintained for the different versions of outputs produced during the human-AI collaborative process?

7. How is evidential disclosure managed in criminal proceedings where AI systems are used in processing and analysing forensic audio, textual data, or other forms of evidence?

Not used at present, but it would need to comply with the AI Usage Policy, as well as forensics legislation and best practice.

I. Please specify the nature of materials disclosed to defence teams (e.g. final transcript only or detailed version history; original audio; AI model metadata etc?
II. Are the documentations of CoC and/or AT disclosed to the defence team? If yes, in what format is this made available?
III. Is there a standard procedure or checklist governing this? If so, please provide a copy or reference it.

8. Has your force conducted any evaluations or assessments regarding the effectiveness of AI systems for evidence processing, including audio, textual, or other forms of evidence? If yes, please provide copies of these documents or reports.

We ran a trial to test the use of AI for object recognition. There has been AI technology used. The technology was deployed over a 3 day period in 2024. Whilst the technology was deployed, there were a total of 65 offences detected, focusing on seatbelt and mobile phone offences. Human intervention reviewed all images and discounted any that did not meet the evidential threshold.

Glossary

***Artificial Intelligence (AI): This refers to a machine that learns, generalises, or infers meaning from input, thereby reproducing or surpassing human performance. The term AI can also be used loosely to describe a machine's ability to perform repetitive tasks without guidance.**

***Audit Trail (AT): Refers to the documentation processes that capture, record, and report the sequence of actions applied to digital evidence. An AT may include details such as model configurations, parameters used, error rates, human interventions, and system-generated logs. It functions as a transparency mechanism, enabling the reconstruction and evaluation of how evidence has been processed, analysed, and interpreted.**

***Automatic Speech Recognition (ASR): A subfield of AI that processes spoken human language (audio) and converts it into written text, useful for tasks like transcription and speaker diarisation.**

***Chain of Custody (CoC): This is the record of how evidence is handled from the point of collection through processing to presentation in court. This may include the identity of the person handling the evidence, date/time of transfer, storage details, and digital identifiers. Alternative terms include 'continuity', 'chain of evidence' and 'provenance'.**

***Forensic Audio evidence: This refers to recorded sound collected, preserved, and analysed for legal or investigative purposes. This often includes spoken language from sources including body-worn cameras, dashcams, police radio communications, and interview or interrogation recordings.**

***Forensic Textual evidence: This refers to written or encoded content, stored or transmitted in digital form, collected, preserved, and analysed for legal or investigative purposes. It includes unstructured human language (e.g., transcripts, emails, chat logs, social media posts), semi-structured data (e.g., system or network logs, ASR outputs), and structured data (e.g., metadata, timestamps).**

***Large Language Models (LLMs): A type of Natural Language Processing (NLP) system trained on vast amounts of text to perform sophisticated language tasks like summarisation, translation, or text generation.**

***Natural Language Processing (NLP): A subfield of AI focused on the interaction between computers and human (natural) language. It involves programming computers to process, analyse, understand, and generate human language. It is useful for tasks like translation, document generation, summarisation and redaction.**

***Paradata: This refers to information generated as a by-product of human interaction with AI systems during evidence processing. This includes prompts, edit histories, data discards, interaction logs, correction logs, reviewer annotations, parameter adjustments, and iterative outputs. Such records provide traceable documentation of how humans and AI jointly contribute to outputs, supporting transparency and accountability in evidential practice.**

HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

POLICY

AI Usage Policy

Governance:	**Strategic Management Board**		
Document Type:	**Policy**		
Policy Owner:	**Head of Corporate Services**		
Department:	**Corporate Services Business Intelligence**		
Policy Writer:	**Advanced Analytics and AI Lead: …**		
Policy Number:	**037**	**Version:**	**1.1**
Effective Date:	**25/09/2023**		
Recommended Review Date:	**25/09/2024**		

CHANGE HISTORY				
Version No	**Author**	**Changes**	**Ratification**	**Date**
1.1	…	Updated to reflect changes of names of boards and change name from PAMLAI to AI		

CONTENTS

1. WHY IS THIS POLICY REQUIRED?

This policy will

1.1 Reduce the number of risks associated with **P**redictive **A**nalytics', **M**achine **L**earning, **A**rtificial **I**ntelligence, and related technologies (hereinafter referred to as **AI** technology).

1.2 Lower the high level of risk associated with the use of **AI** technology.

1.3 Minimise the danger of large-scale reputational damage experienced by others for not having an appropriate policy in place.

1.4 Ensure that any AI technology in use is created, sourced, and used ethically.

1.5 Ensure that any AI technology used will be *benevolent.*

1.6 Ensure that there is *accountability* for the

- Creation of AI technology.
- Purchase of AI technology.
- Use of AI technology.
- Maintenance of AI technology

1.7 Ensure that any AI technology used is *robust.*

1.8 Help to avoid biases inherent in AI work.

1.9 Help to avoid injecting biases into AI work.

1.10 Ensure compliance with the NPCC guidelines (ALGOCARE).

1.11 Facilitate compliance with UK National, and European legislation.

2. WHO SHOULD USE THIS POLICY?

2.1 This policy should be used by NWP officers, special constables, police community support officers, police staff, volunteers, and anyone under contract to NWP (e.g. agency staff). considering the creation, purchase, rental, use or deployment of AI technology, including the use of AI technology from the public domain.

2.2 This policy includes:

- Direction, together with relevant information outlining how the force should approach the use of AI technologies.
- Procedures for different types of AI work.
- The levels of authorisation for different types and categories of AI work
- Links to relevant documents and guidance.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

It is intended that the process outlined in this AI Ethics policy should start at the initiation phase of any programme or project that will make use of AI technology, or as soon thereafter as it is ascertained that a project will involve the use of AI technology.

The terms **piece of work, proposal** and **project** will be used to refer to the project, programme, or part thereof, for which this policy is being consulted.

The term **process** will refer to the **activities outlined herein**.

This policy should be used in conjunction with the AI ethics code, tick list, and guidance notes:

3.1 The AI Ethics Code

The entire ethics code can be found in Appendix D but the main headings are summarised here to give context:

Summary of Code of Ethics

*When considering the initial, or continued, use of **AI** (**P**redictive **A**nalytics, **M**achine **L**earning, **A**rtificial **I**ntelligence) or other data reliant technologies, in order to maximise the benefits and minimise the associated risks, it is imperative that it not just be ethical, but that it be seen to be ethical i.e. that it be demonstrably trustworthy.*
*To be trustworthy a AI technology must have three qualities, it must be: **B**ENEVOLENT, **A**CCOUNTABLE, and **R**OBUST.*
To demonstrate these qualities there is a minimum set of principles that must be upheld.

TRUSTWORTHINESS
To be trustworthy a AI technology must be benevolent, accountable, and robust:

1. Benevolent
a. Seeks to do good (BENEVOLENCE: Purpose)
b. Is free from prejudice (BENEVOLENCE: Fairness)
c. Respects privacy (BENEVOLENCE: Privacy)

2. Accountable
a. Adheres to the law and regulations pertaining to its use (*ACCOUNTABILITY*: Lawfulness)
b. Must not deceive, deliberately or otherwise (*ACCOUNTABILITY*: Honesty)
c. Is subject to continued external oversight (*ACCOUNTABILITY*: Scrutiny)
d. The method for decision making can be explained (*ACCOUNTABILITY*: Transparency)

3. Robust
a. Is reliable (ROBUSTNESS: Reliability)
b. Keeps data secure (ROBUSTNESS: Security)
c. Corrects bias (ROBUSTNESS: Unbiased)

The principles derived from the qualities required for trustworthiness can be further broken into several tenets to test the ethics of any piece of work connected to AI technology. The breakdown can be found in the Appendix D.

3.2 The AI Ticklist can be found in Appendix E

3.3 The AI Use Case and Guidance can be found Appendix F

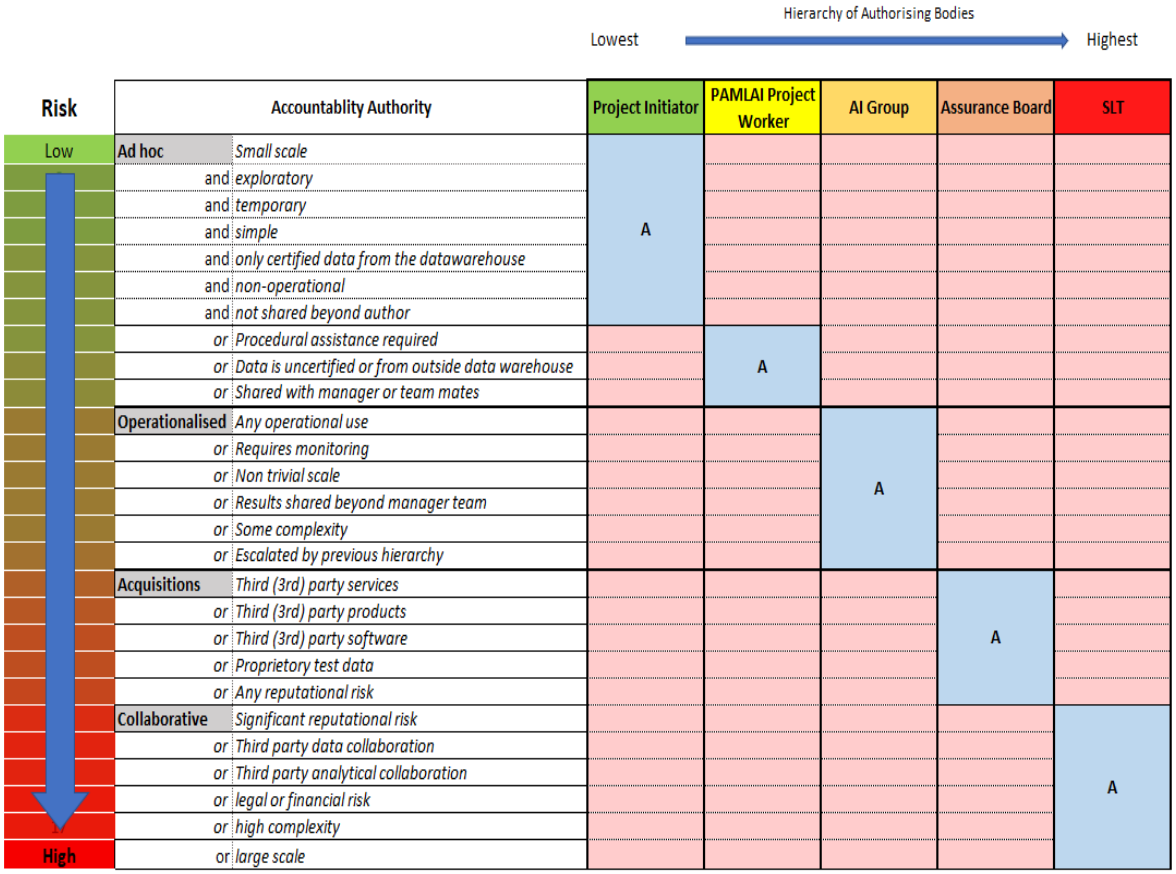
This policy, the AI ethics code, Ticklist, and guidance notes will be available in both English and Welsh versions.

4. ROLES AND RESPONSIBILITIES

The authorisation hierarchy can be seen in Appendix A

4.1 AI Ethics Process Initiator	The person or group who initiate the AI Ethics policy process with a proposal for a project or programme that involves collaborating on, using, creating, renting, or purchasing some element of AI technology
4.2 AI Facilitator	Carries out first line checks that the process initiator has considered the ethicality and full ramifications of the proposed work and can authorise some work (up to level 2). The AI Facilitator will be able to speak Welsh at level 3 or above.
4.3 AI Ethics Group (AIG)	Has oversight of the work carried out by the initiator and facilitator, and can authorise some work (up to level 3)
4.4 Assurance Board	Has oversight of the work carried out by the initiator and facilitator, and AIG and can authorise some work (up to level 4)
4.5 Senior Management Board	Overall authorisation of high risk, complex, and collaborative projects (level 5)

AI projects generally fall into one of four categories, each being associated with different levels of risk. The level required to authorise each type of work is shown in the diagram below, along with a list of criteria that define what fits into each category:



5. THE PROCESS

At the outset of every programme or project a self-assessment must be made by the originator of the piece of work as to whether it will use any AI technology. If it will then, the AI Ethics policy process (hereafter referred to as the process) will need to be followed. Likewise, if a publically available tool uses AI technology then the process should also be followed.

The process begins with an assessment, by the project's originator, of the category of work being undertaken. The authorisation hierarchy matrix should then be used to determine the level of authorisation required. Assistance may be sought from the AI facilitator in this assessment.

The request will flow through the authorising bodies as in Appendix A. the process is designed to be iterative to enable feedback to be incorporated in order to facilitate the authorisation of acceptable proposals

If authorisation is required or desired, then the piece of work will be registered using the AI registration form (see Appendix G)

The process should be followed for each part of the proposed project that uses a different AI technology or that uses the same types of AI technology for different tasks.
e.g. a large programme involving text analysis for summarising statements, text analysis for sentiment analysis, facial recognition should assess the ethicality of each technology and use combination i.e. 3 items to consider in this example.

The AI Ethics Policy Process begins once it is noticed that there will be some element or use of AI technology involved in any given project.

The actions for each role in the process are listed below. A detailed visual process map can be found in Appendix C

5.1 AI Process**: Initiation**

Role	Action Required
5.1.1 Proposal Initiator	Use the AI Ethics code and Ticklist to determine whether the work should proceed, and if so, then register the proposed work using the online form (see Appendix G)
5.1.2 Proposal Initiator	Use the AI Authorisation Matrix to determine whether authorisation is required.
5.1.3 Proposal Initiator	Ask the AI Facilitator for guidance on how to use the Ticklist if desired.
5.1.4 Proposal Initiator	If guidance is desired, submit a request to the AIG using the online form with a partially completed AI Ticklist.
5.1.5 Proposal Initiator	Use the AI Authorisation Matrix to determine the required authorisation level.

5.1.6	Proposal Initiator	Submit the completed AI Ticklist to the AIG.
5.1.7	Proposal Initiator	Await response
5.1.8	Proposal Initiator	Amend the proposal as required by a more senior authorising body.
5.1.9	Proposal Initiator	If authorised, proceed with the proposal under the oversight of the AIG

5.1 AI Process**: Guidance**

Role		Action Required
5.1.10	AI Project Facilitator	Upon receipt of a request provide guidance to the proposal initiator.
5.1.11	AI Project Facilitator	Use the AI Ethics code and Tick-list to determine whether the work should proceed.
5.1.12	AI Project Facilitator	Use the AI Authorisation Matrix (Appendix B) to determine what level of authorisation is required or refer to the AI facilitator.
5.1.13	AI Project Facilitator	Recommend required changes to the project proposal.

5.2 AI Process: **Oversight, Authorisation, or Escalation**

Role		Action Required
5.2.1	AIG (Artificial Intelligence Group)	Each member of the AIG will interpret the AI Ethics code and Ticklist in the light of their own domain of expertise (legal, technical, operational, compliance etc) and the AI guidance notes to determine whether the request should proceed.
5.2.2	AIG	Where there is difficulty in determining whether the request should proceed, the AI Board should gather the opinions of appropriate experts, and use the insights gleaned to interpret the AI Ethics code and Ticklist to determine whether the request should proceed.
5.2.3	AIG	Where necessary request amendments from the Proposal Initiator
5.2.4	AIG	If, based on the AI Authorisation Matrix (Appendix B)or situational judgement, a higher level of authorisation is required or desired, forward the proposal, Ticklist and notes to the Assurance Board

5.3 AI Process: **Authorisation or escalation**

Role		Action Required
5.3.1	AB (Assurance Board)	In the light of the information gleaned from the AIG investigation, AI Ticklist, Ethics Code, and Guidance Notes, determine whether the work should proceed.
5.3.2	AB	Where there is difficulty in determining whether the work should proceed, request AIG gather further information from appropriate experts and resubmit once the fresh information is gathered
5.3.3	AB	Where necessary request amendments from the Proposal Initiator
5.3.4	AB	If the proposal is fundamentally unsound, end the proposal

5.3.5	AB	If based on the Authorisation Matrix, or situational judgement a higher level of authorisation is required or desired, forward the proposal, Ticklist and notes to the Senior Management Board (SMB)

5.4 AI Process: Authorisation

Role		Action Required
5.4.1	SMB (Senior Management Board)	In the light of the information gleaned from the AB, AIG investigation, AI Ticklist, Ethics Code, and Guidance Notes, determine whether the work should proceed.
5.4.2	SMB	Where there is difficulty in determining whether the work should proceed, request AIG gather further information from appropriate experts for resubmission once the fresh information is gathered
5.4.3	SMB	Where necessary request amendments from the Proposal Initiator
5.4.4	SMB	If the proposal is fundamentally unsound, or undesirable, then reject the proposal
5.4.5	SMB	Authorise the work

6. DECLARATION & LEGALITIES

6.1 In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall, the intention of this policy is to make North Wales the safest place in the UK.

6.2 In the writing of this policy cognisance has been taken of the college of policing code of ethics (2014) and proposed revisions (2023).

6.3 North Wales Police policies will be written in accordance with the approved corporate format and published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.

6.4 The following main legal requirements and regulatory have been identified within this policy:

- Equality Act 2010
- Human Rights Act 1998
- The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
- Data Protection Act 2018 (schedule 8) (UK GDPR)
- Freedom of Information Act 2000
- Health and Safety Act 1974
- The General Data Protection Regulation 2016/679
- Data Protection and Digital Information (No. 2) Bill March 2023
- CDDO Algorithmic Transparency Recording Standard
- European Convention on Human Rights (ECHR)
- EU Artificial Intelligence (AI) Act 2021

6.5 Recommendations from following bodies have been consulted for this policy:

- Centre for Artificial (CAIDP) and Office for Artificial Intelligence
- CAIDP, UNESCO, ELI CDDO, CDEI recommendations
- European Law institute (ELI)
- Central Digital and Data Office (CDDO)

- Centre for Data Ethics and Innovation (CDEI)
- Privacy international
- National Institute of Standards and Technology (NIST)
- Royal United Services Institute (RUSI)
- National Police Chiefs Council (NPCC)
- College of Policing (CoP)

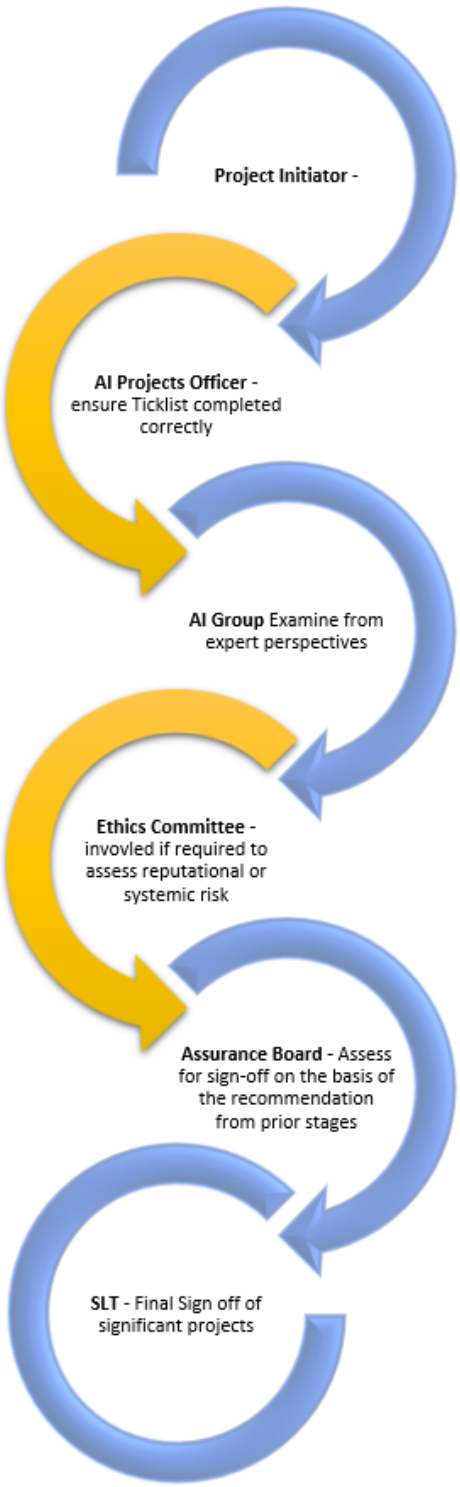
6.6 This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA) and a Welsh Language Impact Assessment (WLIA).

6.7 The area of AI ethics laws, regulations, and recommendations is very active, and changes are expected to be frequent. Changing legislation and deeper understanding of the topic will necessitate regular reviews of this policy document to ensure continued compliance and best practise.

7. APPENDICIES

7.1 Appendix A – Authorisation Levels

The proposal will be considered by the following bodies in the order shown below to the level required according to the Authorisation Matrix (Appendix B). The steps in yellow are only required in some cases.

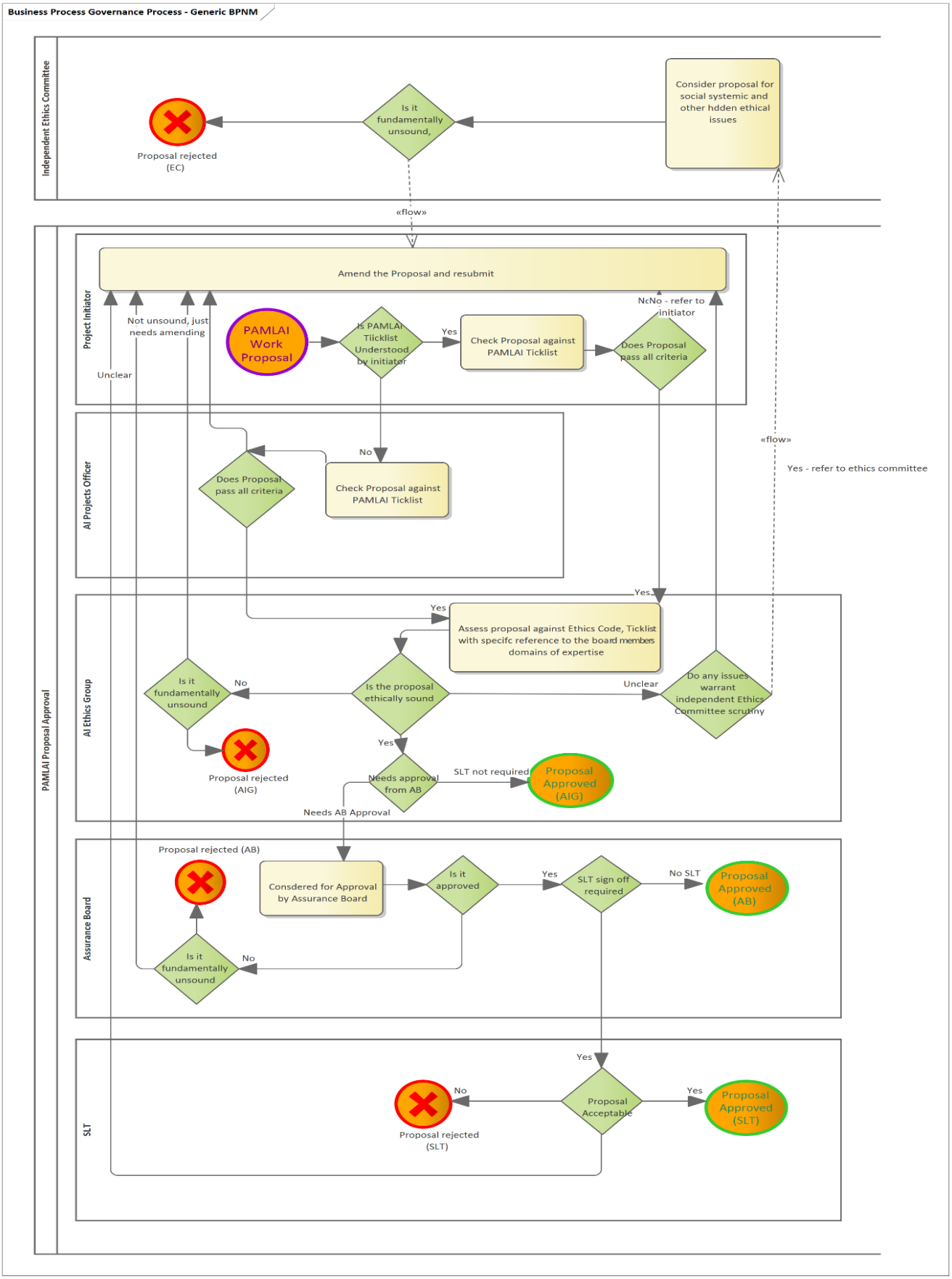


7.2 Appendix B - Authorisation Matrix

Hierarchy of Authorising Bodies: Lowest → Highest

Risk	Accountablity Authority		Project Initiator	PAMLAI Project Worker	AI Group	Assurance Board	SLT
Low	Ad hoc	*Small scale*	A				
	and	*exploratory*					
	and	*temporary*					
	and	*simple*					
	and	*only certified data from the datawarehouse*					
	and	*non-operational*					
	and	*not shared beyond author*					
	or	*Procedural assistance required*		A			
	or	*Data is uncertified or from outside data warehouse*					
	or	*Shared with manager or team mates*					
	Operationalised	*Any operational use*			A		
	or	*Requires monitoring*					
	or	*Non trivial scale*					
	or	*Results shared beyond manager team*					
	or	*Some complexity*					
	or	*Escalated by previous hierarchy*					
	Acquisitions	*Third (3rd) party services*				A	
	or	*Third (3rd) party products*					
	or	*Third (3rd) party software*					
	or	*Proprietory test data*					
	or	*Any reputational risk*					
	Collaborative	*Significant reputational risk*					A
	or	*Third party data collaboration*					
	or	*Third party analytical collaboration*					
	or	*legal or financial risk*					
	or	*high complexity*					
High	or	*large scale*					

7.3 Appendix C – Detailed Process Map



7.4 Appendix D – AI Ethics Code

Embedded File

PAMLAI Ethics Code (PEC) v0.4 - English .

7.5 Appendix E – AI Ticklist

Embedded File

PAMLAI-Ticklist (PET) v0.3 - English.c

7.6 Appendix G – Sample Registration Form

Example of registration form - fill

7.7 Appendix H – Terminology

The following abbreviations are used

Term	Meaning
AI technology	**P**redictive **A**nalytics', **M**achine **L**earning, **A**rtificial **I**ntelligence, and related technologies
SMB	Senior Management Board (highest authorising body)
AB	Assurance Board – policy based decision making board
AIG	Artificial Intelligence group - Deals with AI matter s including the ethicality of proposals
PF	AI facilitator – AI / Ethics expert capable of providing guidance to those using the AI Ticklist
PI	Proposal initiator – the individual or group making the proposal