HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Response Date:04/11/2026

2026/1070 - AI Force Usage

In response to your recent request for information regarding;

Please provide the following recorded information held by the force.
Definition. In this request, 'AI tool' means any software that uses machine learning, a large language model, generative AI, predictive analytics or automated decision support. This includes AI features built into general products (for example Microsoft Copilot or ChatGPT) and data analytics platforms (for example Palantir). It covers tools in live use, in pilot, or used at any time since 1 January 2023.
Scope. I am not asking you to create new information, review individual cases or collate figures. I am asking for existing documents, registers and lists. Please exclude College of Policing guidance. I am not seeking operational detail about investigative or intelligence techniques, and any redaction can be applied at the narrowest level.
A. AI used internally in relation to officers and staff

Not used in this way

For example workforce monitoring, integrity screening, vetting, professional standards, attendance, rostering, performance management or HR.
1. Whether the force uses, or has piloted since 1 January 2023, any AI tool for these purposes. If so, please state the product name, the supplier, the go-live date, and whether it is live or a pilot. Please also say whether the tool forms part of a national or regional framework or pilot.
2. The Data Protection Impact Assessment (DPIA) for each tool, including any updates or reviews.
3. The Equality Impact Assessment (EIA) for each tool. If none was completed, please confirm this in writing.
4. The terms of reference, or equivalent governance document, for any unit, board or group that oversees each tool.
5. Any internal policy, standard operating procedure or guidance on how outputs are used, how human review is applied, and how use of the tool is monitored and audited. Please include the most recent audit or review report, if one exists.
6. The contract value and the annual licence or running cost for each tool. A link to a published contract notice is acceptable.
7. Whether staff associations or trade unions were consulted before each tool was deployed, and any record of that consultation.

B. AI used by officers and staff in their work, internal and external-facing.
The following use cases are in planning but not yet live:
Transcription – no DPIA
Summarisation – no DPIA
Redaction – DPIA attached

There is one case in use; a training tool that used an AI avatar as a training tool to improve interviewing of victims. The DPIA is attached.

Harm has been identified in providing you with the full redaction DPIA, data relating to security measures, processor details, diagrams, risk and software as this information could make us susceptible to cyber breaches, we will conduct a public interest test to decide on disclosure;

The exemptions and data being considered in the public interest test are listed below:

Section 31 (1) Law Enforcement

Section 31 is qualified prejudice-based exemption which means that the public authority must demonstrate that it is satisfied that to release the information would hinder our own law enforcement. The public authority must consider the balance of the public interest in releasing the information against the public interest in withholding it.

To provide details of security measures, processor details, diagrams, risk and software can have a significant potential for the law enforcement position to be undermined.

Harm Test

Section 31
With information about the security measures, processor details, diagrams, risk and software, it becomes easier for any hacker to gain access to the system. Which would be detrimental to our day-to-day operations.

Public Interest Test

Factors Favouring Disclosure section 31

There is a strong public interest in public authorities being open and transparent and disclosing data relating to the systems we use and how we use them assists with this.

Factors Favouring Non-Disclosure section 31

There is a significant potential for the law enforcement position to be undermined if the security measures, processor details, diagrams, risk and software is revealed. This information would be used by hackers to gain access to the system, which would have a significant impact on our day-to-day activities and operations.

Balancing Test

There are factors which in general terms favour release of this information, however, the factors favouring non-disclosure are more specifically relevant.

We cannot disclose information which would put our Force at risk or create security issues for us.

My decision, therefore, is not to release this information.

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

For example generative AI assistants, transcription, summarisation, drafting, redaction, call triage and public-facing chatbots.

8. Any register or list of AI tools that have been authorised, procured or piloted. If no single list is held, a list of the titles of DPIAs that relate to AI tools will be sufficient.
MLOps platform c.100 allowing us to build our own AI solutions and run them in house.
Transcription and redaction are underway.

9. The DPIA and the EIA for each tool listed at item 8.
Speak yto information assurance about DPIAs and to Diversity about EIA
10. Local policy or guidance on acceptable use of AI by officers and staff, including any rules on unapproved tools. Or confirm there is no guidance.
The current policy is attached, please note, is it currently under review to cover ongoing changes in AI.

11. The training materials provided to officers and staff on the use of AI, or a description of their content. Please say whether the training is mandatory.
Training has been provided to all Senior Management Teams on the risks and dangers of AI. It will soon be re-run.

12. Guidance or policy on how AI use is logged, monitored and audited, and the most recent audit or review report. Or confirm that there is no guidance, policy or audit process.
A new AI audit procedure is being currently being created.

13. The contract value and the annual licence or running cost for each tool listed at item 8.
As the use cases are still in the planning stage there are no contracts, licence or running costs.
A Home office grant has used and usage is free.

14. The terms of reference for any AI board, ethics group or senior oversight forum, and the date it was established. Or confirm the board does not exist
Artificial Intelligence Governance Board did control the use of AI, however, this has recently been stood down, there is a plan of incorporating the work into the Information Security board.

Having disclosed high-level information about routine, non-sensitive uses of Artificial Intelligence (AI), North Wales Police *will neither confirm nor deny* whether it holds any further information that would indicate whether AI is, or is not, used in connection with counter-terrorism, serious and organised crime, covert intelligence activity, or specialist digital forensics supporting those functions. The duty to confirm or deny is disapplied by virtue of sections 24(2) (national security) and 31(3) (law enforcement) of the Freedom of Information Act 2000. This response should not be taken as an indication of whether any additional information is held.

Confirming or denying whether AI is used by North Wales Police in counter-terrorism, serious and organised crime, covert intelligence or specialist digital forensics would enable hostile actors to infer the presence, absence or maturity of particular policing capabilities. This type of capability insight is of practical value to adversaries who routinely adapt their behaviour to exploit perceived weaknesses, overwhelm less technologically equipped forces, or adjust methods to avoid detection. Even a single confirmation or denial could be combined with publicly available information from other forces to build a detailed national picture of capability. This mosaic effect represents a realistic and actionable risk, providing information that could materially undermine national security and the effectiveness of law-enforcement operations.

Public Interest Test – Section 24(2) (National Security)

Factors in favour of confirming or denying - There is a strong public interest in openness and transparency about the use of AI in policing. Confirming or denying the existence of information could contribute to informed public debate about how emerging technologies are deployed, the safeguards in place, and whether they align with legal and ethical standards. Disclosure can enhance accountability, promote trust, and reassure the public that AI use is subject to appropriate oversight.

Factors against confirming or denying - There is an overriding public interest in protecting national security. Confirming or denying the existence of information about AI deployment in CT, SoC, covert intelligence, or linked specialist forensics would provide adversaries with useful insights into operational capabilities and priorities. Even a simple confirmation or denial could enable hostile actors to adjust methods, exploit potential gaps, or test thresholds. The resulting risk to national security would be real and more than trivial, and is not mitigated by partial or local confirmations, because the cumulative mosaic effect across multiple forces would still disclose sensitive capability at a national level.

Public Interest Test – Section 31(3) (Law Enforcement)

Factors in favour of confirming or denying - There is a general public interest in understanding how AI is used to support policing functions, including the efficiency and effectiveness of core processes, and in ensuring that novel technologies are used lawfully and proportionately. Confirmation or denial could support external scrutiny and promote confidence in policing practice.

Factors against confirming or denying - Confirming or denying the existence of information relating to AI use in CT, SoC, covert intelligence, or specialist digital forensics would be likely to prejudice the prevention and detection of crime, the apprehension or prosecution of offenders, and the operation of law enforcement tactics and methodologies. Knowledge of whether specific capabilities exist, or do not exist, enables offenders to adapt behaviour, exploit capability gaps, frustrate investigations, and increase the cost and complexity of counter-measures. The public interest strongly favours maintaining an NCND to preserve the effectiveness of law enforcement and the safety of the public.

Balance Test
For the reasons set out above, North Wales Police will neither confirm nor deny whether it holds information indicating AI is used in CT, SoC, covert intelligence activity, or specialist digital forensics supporting those functions.
The public interest in maintaining the NCND position under sections 24(2) and 31(3) outweighs the public interest in confirmation or denial. This response should not be taken as an indication of whether any relevant information is held.
A separate response has already provided high-level information about routine, non-sensitive AI use. To go further would risk disclosing sensitive capability by inference.

This letter acts as a Refusal Notice under section 17 (5) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 02/11/2026

DATA PROTECTION IMPACT ASSESSMENT Screening Form

This document provides information and guidance to help you complete the Data Protection Impact Assessment (DPIA) screening process (page 4 onwards), to determine whether a full DPIA is required.

You will also find further clarification and assistance where you see an '?' situated in the DPIA screening form below, and also examples where you see *(Hover for examples)*.

Please also refer to the ICO guidance when completing this form.

What is a DPIA?

Data protection and privacy must be at the forefront of the design of any new, or changes to, a system, proposal, project or plan.

A Data Protection Impact Assessment (DPIA) is a process designed to help organisations analyse, identify and mitigate data protection and privacy risks. DPIAs also consider broader risks to individuals and/or society. The focus is on the potential for harm (physical, material or non-material).

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether the remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to result in a high risk. However, an effective DPIA can also bring broader compliance, financial and reputational benefits, helping organisations to demonstrate accountability.

What is the DPIA Process?

A DPIA should be considered early in the life of a project (when you know what you want to do and how) and crucially, before you start processing and committing any financial resources.

The DPIA process has two stages:

- **Stage 1: DPIA screening** - the DPIA screening will determine whether a DPIA will be required (i.e. processing is likely to result in a high risk). If you require advice or guidance, please contact the Data Protection Officer on dataprotectionenqs@nthwales.pnn.police.uk

- **Stage 2: DPIA** – This will document a full assessment of the risks and records decisions about the use of personal data.

When is a DPIA is required?

A DPIA will be required when the processing is likely to result in a 'high risk' to the 'rights and freedoms of individuals'.

The Information Commissioner's Office (ICO) have published guidance outlining a number of factors which are likely to present a 'high risk' when processing personal data. These factors are outlined in Section 3 of the Screening Form.

When considering an individual's rights and freedoms, although the primary concern relates to the right to privacy, it may also involve other fundamental rights or lead to physical, material or non-material damage, for example:

- discrimination, identity theft or fraud, financial loss or reputational damage;
- where the vulnerable, children or special categories of data are processed;
- where personal aspects are evaluated in order to profile individuals (e.g. performance at work, health, reliability or behaviour, location or movements);
- where an individual is prevented from exercising control over their data; or
- where the processing involves a large amount of personal data or affects a large number of data subjects.

The DPIA screening will determine whether a DPIA is required.

Who should complete the DPIA Screening and the DPIA?

The head of department/Information Asset Owner (IAO) commissioning the proposal is responsible for ensuring the screening takes place and for ongoing review of a DPIA to ensure that the document is kept current and relevant, ensuring changes to how data is managed are captured. Undertaking of the Screening and DPIA can be delegated to a **designated business lead** or **project manager.**

The Data Protection Officer (DPO) is required within their statutory duties to monitor and advise IAOs on DPIA compliance.
The DPO will review fully completed DPIA Screenings to ensure that the process has been correctly followed and the risks identified.
The DPO will:-

- provide an initial assessment on the fully completed DPIA Screening form;
- provide advice where the project needs to do further work to adequately complete the document and deliver data protection by design and default; and
- provide a final assessment to any revised DPIA Screening as to whether a full DPIA is required.

How should I complete the DPIA screening?

Complete the fields required on the DPIA screening form, avoid technical jargon and acronyms, and ensure you explain the proposal in a way that someone with no prior knowledge could easily understand.

After review by the head of department/Information Asset Owner, submit completed forms to the Data Protection Officer (DPO) via email to dataprotectionenqs@nthwales.pnn.police.uk . Failure to provide sufficient information will delay the Data Protection Officer's assessment and response.

DPIA SCREENING	
Step 1 - GOVERNANCE	
Project Proposal Name:	Project Efa
Head of Department/Information Asset Owner[?]:	…
Designated Business Lead/Project Manager:	Project Resource not yet assigned.
Date on which system/initiative expected to commence:	01/04/2026
Date sent to Head of Department/Information Asset Owner for assessment	DD/MM/YYYY
Date assessment completed by Head of Department/Information Asset Owner	16/10/2025
Date sent to DPO	16/10/2025
Step 2 – OVERVIEW	
2.1 Aim and Purpose: Avoiding technical language and acronyms please provide a brief overview of aim and purpose of the process or proposal, focusing on where personal data will be processed. It may be useful to refer to project documentation and diagrams.	
Project Efa will explore the value of staff interviewing a Gen-AI representation of a real-world stalking victim to improve operational practice. Interviews will automatically be assessed against best-practice standards, resulting in personalised staff feedback and aggregated insights into the organisational response to stalking and how that response can improve. **The innovation of the project consists of using a self-hosted Large Language Model supported by Retrieval-Augmented Generation (RAG) to:** **1. Portray a victim of stalking informed by the personality, characteristics and**	

lived experience of Rhiannon Bragg, a high profile victim-survivor of stalking in North Wales. The AI representation will communicate with users through a text and speech interface and respond naturally to rapport-building and investigative techniques. It will embody a real victim's lived experience and 'voice' for interaction at scale.

2. Assess a large number of resulting interview transcripts against a repository of best practice, including College of Policing Authorised Professional Practice, input from Subject Matter Experts (including victim-survivors) and specific assessment criteria aligned to force policy and procedure to generate thematic insight. Themes will include:
- How do our officers/staff engage and build rapport with victims?
- How effective is their initial investigation and risk assessment?
- How effectively do they reassure victims and signpost them to support services?

3. Provide personalised, objective and consistent feedback directly to a large number of our officers in order to improve their practice, while testing whether AI-enabled assessment for empathy and interviewing standards is an effective means of formative assessment.

4. Support a feasibility study into using Gen-AI roleplay, and the methodological insights and data it is anticipated to generate, as a means of advancing policing knowledge through operational evaluation and audit.

2.2 Explain whether it involves the collection of new information about individuals

☒ Yes ☐ No - already collect ☐ No information about individuals involved

The process will be utilising real accounts from a stalking survivor to educate staff within North Wales Police. This information is held and owned by the private company that delivers the AI based training. The data collected and processed from a NWP perspective would be the dialogue between the AI and the officer undertaking the training. This will be held within the AI environment.

2.3 Explain if it will involve multiple processes
E.g. if it was a HR system it could have multiple processes such as:- Recruitment, Payroll & Pensions, Employee Relations, and Learning & Development all within one system.

☐ Yes ☒ No

Click here to enter text.

2.4 Explain whether a DPIA has been completed previously? (by NWP or another similar organisation).

In the text box, outline whether a DPIA (or PIA) has been completed previously or not. If already a current process, outline whether the nature, scope, context or purpose of the current processing has changed.

☐ Yes ☒ No

Click here to enter text.

Step 3 – PERSONAL DATA USE

3.1 What types of personal data about living individuals will be used?
(select all that apply and provide further detail in the free-text box if required)

☐ None (no personal data)	☐ Suspects	☐ Racial / ethnic origin
☐ Names	☐ Convicted people	☐ Religion
☐ Dates of birth	☐ Victims of a criminal offence	☐ Political opinions
☐ Addresses	☐ Witnesses of offences	☐ Philosophical beliefs
☐ Unique identifiers	☐ Children	☐ Sex Life
☐ Contact numbers	☐ Vulnerable individuals	☐ Sexual orientation
☐ Email addresses	☐ Organisation's staff	☐ Health data
☐ Sound/visual images	☐ Complaint records	☐ DNA samples/profiles
☐ Facial recognition	☐ Criminal records	☐ Blood samples
☒ Lifestyle/Social circumstances	☐ Employment records	☐ Fingerprint data/profiles

The training utilises the lived experience of a stalking survivor within the North Wales Area. They have provided details of their experience with a private company who have developed this training package..

3.2 How will the data be collected?
Briefly outline how you will obtain the data, examples include: directly from individuals, from another data set already in our possession, from a partner agency.

Data already exists within the training package. No new data other than staff/officer responses will be collected by NWP.

3.3 How many people will be affected (yearly basis)? (Select one answer below)

☒ Fewer than 100 data subjects
☐ 100 to 1000 data subjects
☐ 1000 to 5000 data subjects
☐ More than 5000 data subjects

Click here to enter text.

3.4 Will personal data be shared with anyone (select all that apply)

☐ Partners / other agencies
☐ Internal – other departments
☐ Service provider / processor
☐ Shared inside of UK (check Cloud storage)

☐ Shared outside of UK but within EU ☐ Shared with country outside of the EU
3.5 Explain the review, retention and disposal process All records must have a retention period set by the owner of the information when first created or received.
RRD aligned to NSWG guidelines. Subject of annual inspection by IPCO. NWP only hold data that they are legally obliged to hold. All material where retention cannot be justified has been deleted. Regular reviews of data are in place.

Step 4 – SCREENING QUESTIONS

The below are a number of factors that are likely to present a 'high risk' to individuals when processing personal data.
Saying **'yes'** to one or more of the following will indicate that a DPIA is required.

	Does the processing involve:	**'Yes' or 'No'**	**If 'Yes' then please provide further details**
1.	**Systematic? and extensive? evaluation based on automated decision-making? or profiling?, resulting in legal/other significant? effects** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
2.	**Data Processed on a large scale?, and in particular relating to special category data?, criminal data, or of a highly personal nature** *(Hover for examples)*	☐ Yes ☒ No	
3.	**Systematic? monitoring of a publically available area on a large scale?** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
4.	**New technologies? or novel application of existing technologies** *(Hover for examples)*	☒ Yes ☐ No	Unsure if the technology is new as generative AI has been used across policing. It may be that this is one of the first times it has been used to deliver training within policing.
5.	**Denial of service?** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
6.	**Any processing of biometric? or genetic? data** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
7.	**Data matching?:** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
8.	**Invisible processing?** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
9.	**Tracking?**	☐ Yes	Click here to enter text.

	(Hover for examples)	☒ No	
10.	**Targeting of children or vulnerable individuals for marketing, profiling, automated decision-making or the offer of online services.** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.
11.	**Risk of physical harm**[?] *(Hover for examples)*	☐ Yes ☒ No	
12.	**Evaluation or scoring**[?]	☐ Yes ☒ No	Whilst the training will provide feedback it is from a learning and development perspective not a performance one.
13.	**Processing which prevents individuals from exercising their rights or using a service or contract** *(Hover for examples)*	☐ Yes ☒ No	Click here to enter text.

Please complete the Governance Section (Step 1), and the initial assessment by the Head of Department/Information Asset Owner in Step 4, prior to sending to the DPO using the following mailbox:-
dataprotectionenqs@nthwales.pnn.police.uk

Step 4 – IAO ASSESSMENT	
In most cases, only one of these factors indicates the need for a DPIA. However, this is not a strict rule. You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is unlikely to result in a high risk, but you should document your reasons.	
Assessment of IAO (include your rationale for completing/not completing a full DPIA	Based on the above screening I will take guidance from the DPO as only the use of AI seems to suggest that a DPIA will be required.
Assessment completed by:	Name: … Date: 16/10/2025

Step 5 – DPO Review
The DPO will conduct a review of the information provided, and will offer advice on any further work needed on this screening document, and whether a full DPIA is required.

A. A DPIA is not required.	☐	Click here to document rationale.
B. A DPIA is not required as long as the following remedial action listed is carried out. If the remedial action is not carried out, a DPIA will be required.	☐	Click here to document rationale.
C. A DPIA is required.	☐	Click here to document rationale.
Assessment completed by:	Name:	Date:

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? 3

2. WHO SHOULD USE THIS POLICY? 3

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY? 3

3.1 The AI Ethics Code 4

The entire ethics code can be found in Appendix D but the main headings are summarised here to give context: 4

Summary of Code of Ethics 4

3.2 The AI Ticklist can be found in Appendix E 4

3.3 The AI Use Case and Guidance can be found Appendix F 4

4. ROLES AND RESPONSIBILITIES 5

4.1 AI Ethics Process Initiator 5

4.2 AI Facilitator 5

4.3 AI Ethics Group (AIG) 5

4.4 Assurance Board 5

4.5 Senior Management Board 5

5. THE PROCESS 6

5.1 AI Process: Initiation 6

5.1 AI Process: Guidance 7

5.2 AI Process: Oversight, Authorisation, or Escalation 7

5.3 AI Process: Authorisation or escalation 7

5.4 AI Process: Authorisation 8

6. DECLARATION & LEGALITIES 8

7. APPENDICIES 10

7.1 Appendix A – Authorisation Levels 10

7.2 Appendix B - Authorisation Matrix 11

7.3 Appendix C – Detailed Process Map 12

7.4 Appendix D – AI Ethics Code 13

7.5 Appendix E – AI Ticklist 13

*7.6 Appendix F – AI Guidance ..... **Error! Bookmark not defined.***

7.7 Appendix G – Sample Registration Form 13

7.8 Appendix H – Terminology 13

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

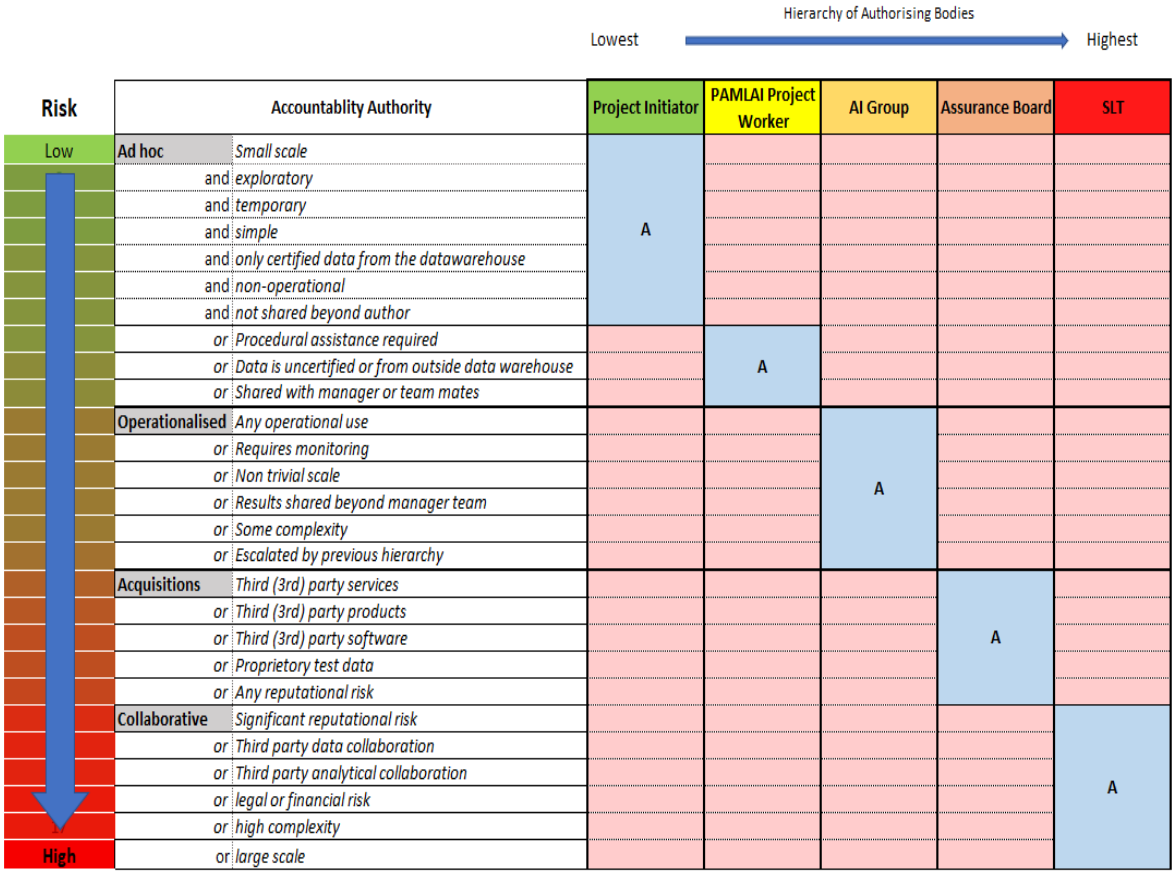
This policy, the AI ethics code, Ticklist, and guidance notes will be available in both English and Welsh versions.

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)

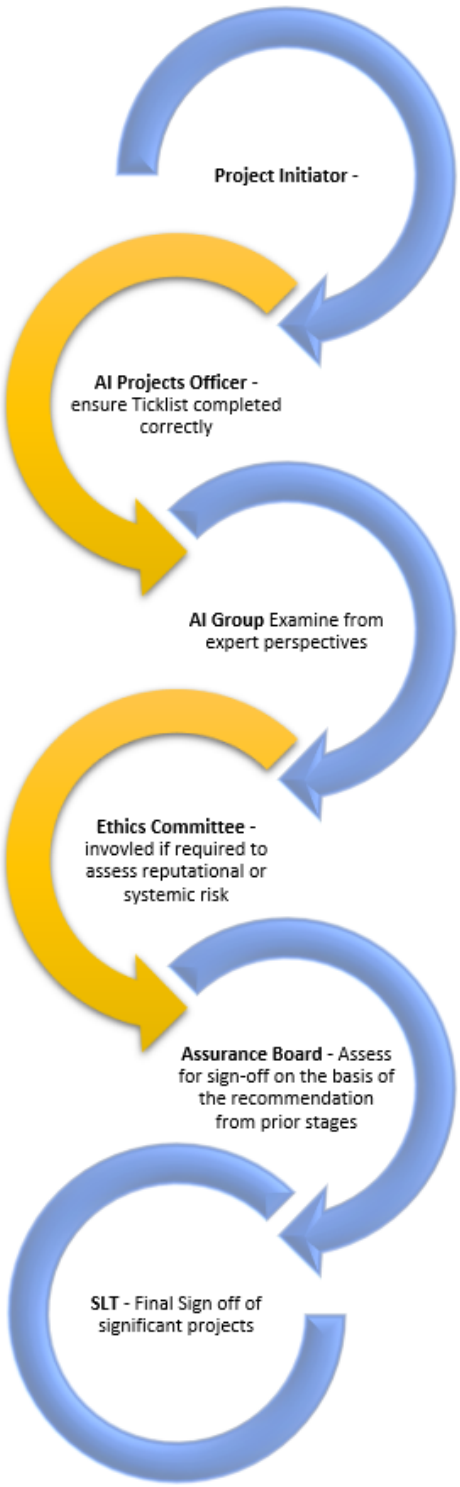
6.6 This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA) and a Welsh Language Impact Assessment (WLIA).

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.

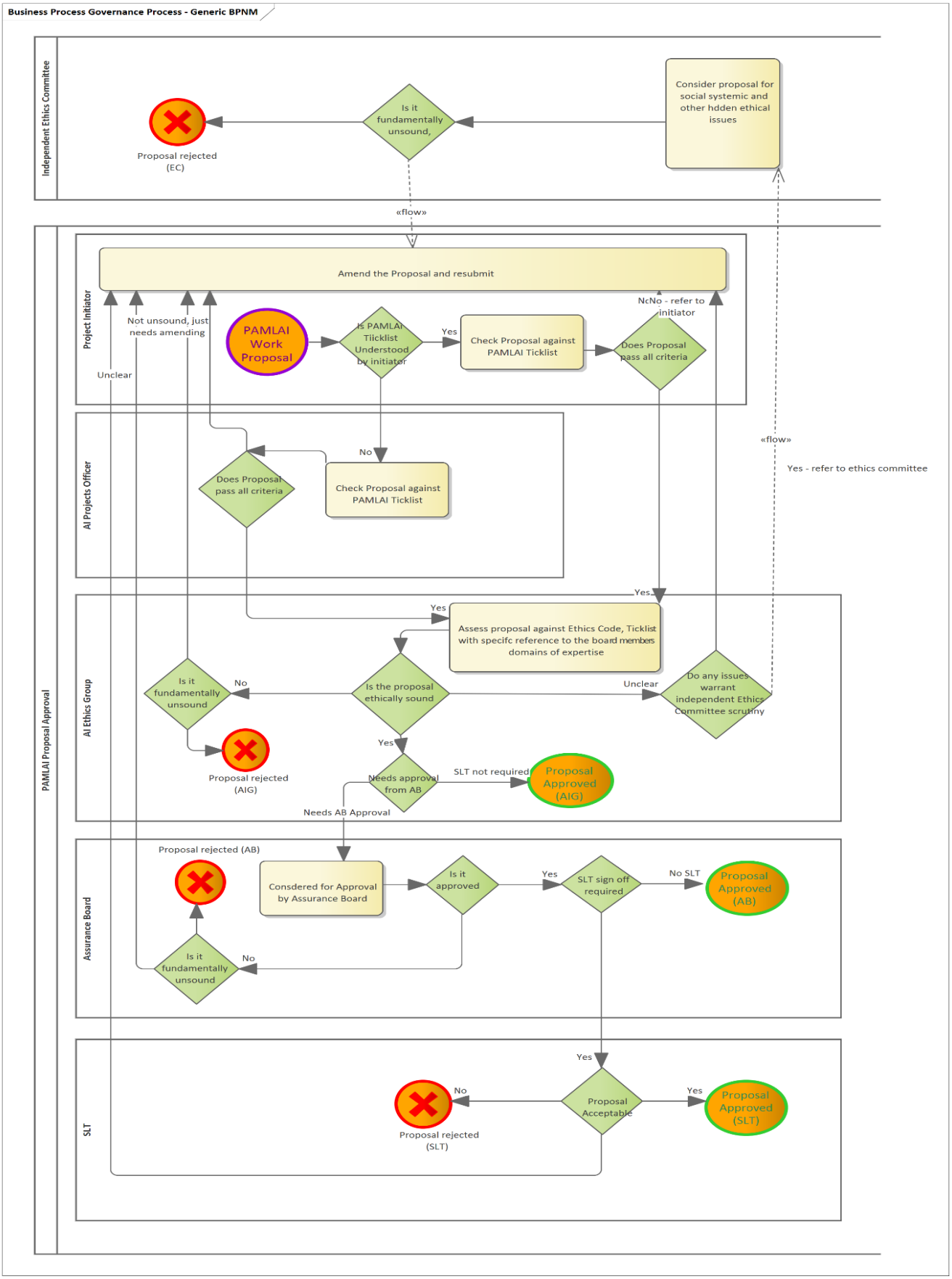


7.2 Appendix B - Authorisation Matrix

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

DATA PROTECTION IMPACT ASSESSMENT

This document enables you to complete a full Data Protection Impact Assessment (DPIA), if your Screening Form indicates that one is required.

Within the form below, you will find further clarification and assistance where you see a '**?**'.

Please also refer to the ICO guidance when completing this form.

How to complete this form?

In this stage of the DPIA process you must provide full details about the context, necessity, proportionality and risks associated with the proposal. It will supplement the information provided in the DPIA screening document.

The aim of this process is to identify and mitigate risks and to consult the Information Commissioners Office (ICO) (before processing commences) where residual risks to individuals are high.

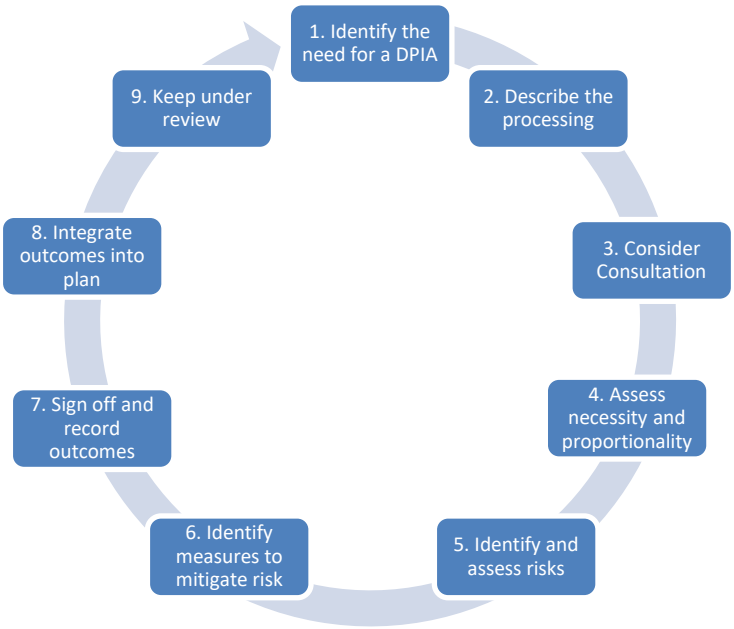
Data Protection legislation and the ICO set out essential requirements that must be addressed within a DPIA. These are incorporated into the form so it is vital that you fully complete every step (where relevant).

Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.

If you require advice or guidance, please contact the Data Protection Officer on dataprotectionenqs@northwales.police.uk

In the event of a residual risk remaining 'high', the Head of Department/Information Asset Owner must refer this DPIA to the Data Protection Officer (DPO) on dataprotectionenqs@northwales.police.uk and then following the DPOs advice, the DPIA will be referred to the Chief Information Officer/SIRO to accept the risk prior to referral to the ICO.

Below is an example of the DPIA lifecycle:



DATA PROTECTION IMPACT ASSESSMENT (DPIA)	
Project Proposal Name:	Audio Visual MultiMedia Redaction (AVMMR)
Head of Department/ Information Asset Owner[?]:	… Head of Change and Collaboration
Designated Project Manager:	…
Date on which system/initiative expected to commence:	02/02/2026
Date sent to Head of Department/Information Asset Owner for assessment:	15/12/2025
Date assessment completed:	15/12/2025
If any residual risks remain High	
Date sent to Data Protection Officer:	DD/MM/YYYY
Date sent to CIO/SIRO:	DD/MM/YYYY
Date sent to ICO:	DD/MM/YYYY

Step 1: IDENTIFY THE NEED FOR A DPIA
1.1 Using the DPIA screening document, summarise the need for a DPIA (Include which screening criteria flagged the processing as likely to be high risk).

The CPS have set out a new requirement in the Directors Guidance 6th edition for case builds which calls for the redaction of documents including text, video and audio. This is currently done manually for video and audio and as such is incredibly labour intensive and slow.

The Pimloc – Secure Redact tool has been selected as an affordable, configurable solution to aid with the above but also allows investigating officers to upload police generated video footage (body worn, dashcam, officer mobile, Force CCTV etc) and blur out faces of those not relevant to evidential capture and subject to collateral intrusion. The DFU department will use it to redact any non police generated footage. The solution will also allow officers to track an individual (not in live/real time) based on a qualifying item. For example, 'man in red shirt' or by highlighting the subject to be tracked. The solution will also enable officers and staff to redact police generated video footage to suit requirements eg FOI requests. The DFU and imaging specialists will be able to use it for all external footage (CCTV, mobile phone, doorbell etc).
The application will be able to take in many hours of footage from all social media platforms, CCTV, BWV and smartphones. It will then have the capability to identify an individual, and trace them throughout all the footage, which will then give a fuller picture of any actions that individual has taken. This will be of use within any violent disorder or mass brawls or major crime investigations etc.

PimLoc – Secure Redact – Video analytics software – Is also currently being trialled in South West Forensics (D&C) as well other forces nationally. They are also working with NICE for integration – who are the provider of our DEMS solution.

Initially, the system will be setup and used over 12 months with a set period of hours available. Teams in mind to use this will be DFU, DIT, FMIT, IA, DA, JS and PVPU

The necessary documentation from the supplier Pimloc can be found below:
- Pimloc - Pimloc Home Page
- Privacy Policy — Pimloc

1.2 Project aims and purpose? • *What do you want to achieve?* • *What is the intended effect on individuals?*	To be able to autmatically redact all identifying information within video footage and anonymise individuals in clips which may be required for a variety of uses e.g. subject access requests, civil case requests, media requests etc. It will also enable compliance with the CPS Directors Guidance 6th edition for case files and evidence.
1.3 Benefits of the processing • *What are the benefits to the organisation, individuals, public?*	Secure Redact automates many of the repetitive redaction management tasks that are perform manually • Saving time for NWP on each investigation by finding redacting faster • Protecting data and images of people / items that need to be redacted – more accurately than a manual process would

	The software will not be used to identify an individual (like facial recognition would) and will only be used to track and weed out those suspected of being involved in criminality so that images can be gathered for investigation and intelligence purposes. ie. it allows investigators to find a known individual (based on their clothing / head covering / face) across footage – but it does **not** identify who they are (eg. Paul Smith). The detections are also used to provide redaction so that individuals can be anonymised in video clips, which may be required for a variety of uses (ie. subject access requests, civil case requests, media requests etc) Automatically blur faces, heads and license plates in video streams and batch files at scale, for incidents and data compliance.

Step 2: DESCRIBE THE PROCESSING AND FLOW OF INFORMATION

This section outlines the **nature**, **scope**, and **context** of the processing.

Please describe how and why you plan to use the personal data in as much detail as possible, including reference to the high risk processing identified in the screening.

2.1 Nature of the processing

2.1.1 Stage of processing	Description
Collection Where does the data originate from (sources), who will collect it, how will it be data obtained and how often?	Data has already been collected per existing practices into existing systems for the purpose of conducting a criminal investigation. This could be any digital video gathered in an investigation ranging from (but not limited to) social media downloads, dashcams, Doorbell's, submitted videos, BWV, cloud-based data, and CCTV
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	The data will be analysed and redacted by Secure redact …. The outcome is to drastically speed through the manual redaction step the investigators currently have to complete using software

Access Describe who has access to the data throughout the life of the processing.	Technology / CGI - Enabling remote access for install. Supplier - … CTO (NPPV3 / SC), if provided explicit permission from NWP, can gain root access to customer data if required NWP Training Investigators (Data confidentiality NPVV3 vetted) Responding to NWP Investigators about how to use the software. Users – Users identified for the trial will have access to the data they upload and redact per their cases.
Processors Describe the use of processors. If a third party is used, is a contract in place to regulate the relationship? Will any personal data be processed outside of the UK or the EU?	….
Sharing Will you be sharing the data with anyone? If so, what will you share, why, and who will receive it? (Sharing could be external or internal to the organisation, national or international).	No External sharing of data will occur directly from Pimloc. The redacted files will be shared via existing processes to external parties such as the CPS. Sharing with NWP in line with current processes and policies https://www.secureredact.ai/privacy-policy
Review, retention, disposal Describe your plan for review and retention (e.g. how long you will keep the data), linking to the organisations' retention schedule where appropriate. Also, describe the process for disposal of data, including when and how.	All data will be deleted at the completion of the trial/contract. All electronic records will be purged from the Pimloc SecureRedact system and the system destroyed (deleted). Please note this is in reference to the trial instance and copy of data – the source systems and data will remain intact. If we proceed with the software after the initial funded use, then we will set an automated retention and disposal procedure with SecureRedact. This will be for Pimloc to automate automatic deletion of all data older than 60 days.
Security measures Describe how you will keep personal data secure.	…
2.1.2 Storage and Assets Describe where and how the data is to be stored including the assets you intend to use.	
Asset	**Description**
Hardware	…

	Police issued laptop / desktop, Microsoft (Azure)
Software	…
Networks	…
Hardcopy/paper	n/a
Any other relevant assets	NiCE DEMS for redacted files storage

2.1.3 Diagrams and tables

If you have a diagram or table which describes or demonstrates the processing (and information flows), please include it below.

…

2.2 Scope and context of the processing

2.2.1 Will the processing involve law enforcement[?] data or general data?

(Please select below)

☒ Personal data processed for law enforcement purposes

☐ Personal data processed for general (non-law enforcement) purposes

2.2.2 What categories of individuals will be involved?

(Please select all applicable categories below)

☒ Persons suspected of having committed or being about to commit a criminal offence

☒ Persons convicted of a criminal offence

☒ Persons who are or may be victims of a criminal offence

☒ Witnesses or other persons with information about offences

☒ Organisations' staff (current and former)

☐ Other

If other, please provide further details below:-

Click here to enter text.

2.2.3 What types of personal data will be processed?

Provide an overview of the categories of personal data that will be processed, for example: names, DOB's, addresses, vehicle registration plate number, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

The data being processed is Operational Data that is seized by Police for a criminal investigation. The data may contain:

- Racial or ethnic origin information
- Political opinions
- Religious or philosophical beliefs

- Trade union membership
- Biometric data
- Health
- Sex life
- Sexual orientation

During a criminal investigation, digital evidence such as: mobile phone(s), computer(s), telephone records, bank records, CCTV footage, etc. may be acquired and analysed. It is routine to encounter various personal (sensitive) data in this digital evidence; that data will then become part of that criminal investigation.

The footage can include multiple factors that needs redaction, such as other persons, names, location, vehicles, etc. It can also relate to children and the vulnerable. This DPIA is only concerned with the processing requirements of Pimloc and not the capture and retention of the actual footage.

Whilst maybe not meant in the spirit of Special Category Data, it is important to note that individuals will be identified, or looked, at based on physical appearance. It may be that a subject is identified committing a crime and the footage shows a white male therefore a male will be tracked on footage based on race. Video footage includes the physical appearance of individuals which can encode a variety of special category data in the form of clothing, head coverings, insignia/badges, locations, associations, actions etc

2.2.4 How many data subjects will the processing affect?
(Please specify one answer below)

☐ Fewer than 100 data subjects
☐ 100 to 1000 data subjects
☐ 1000 to 5000 data subjects
☒ More than 5000 data subjects

2.2.5 Will you be processing any special category or criminal data?
(Please specify one or more answers below)

☒ Race or Ethnic origin	☒ Trade union membership
☒ Political opinions	☒ Genetic or Biometric Data
☒ Religious or Philosophical beliefs	☒ Sex life / Orientation
☐ Criminal convictions/offences	☒ Health

2.2.6 Will the processing include data about children or other vulnerable people?
Please provide details in the text box.

☒ **Yes** ☐ **No**	It is possible that during a criminal investigation, data will be processed that relates to children and vulnerable people. They may appear in videos and evidence; this will not be known until each is reviewed but is extremely likely.

2.2.7 Your relationship with the individuals:

Describe your relationship with the individuals who are subject to the processing. Are they likely to expect the processing? Outline the extent to which they will have control over their data.	
During a criminal investigation, digital evidence such as: mobile phone(s), computer(s), telephone records, bank records, CCTV footage, etc. may be acquired and analysed. It is routine to encounter various personal (sensitive) data in this digital evidence; that data will then become part of that criminal investigation. The data subject will be informed by NWP of processing via the NWP privacy notice. The data subject has a right to request to see what data is held through a subject access request.	
2.2.8 Has personal data been processed in a similar way previously? Please provide details in the text box.	
☒ **Yes** ☐ **No**	**T**his data is currently being processed in the same way for the purpose of investigating criminal offences. Video data is currently redacted manually
2.2.9 Have you considered any approved codes of conduct, certification schemes or codes of practice?	
☒ **Yes** ☐ **No**	**T**he following have been considered: The Data Protection Act 2018 (as the UK's implementation of the General Data Protection Regulation (GDPR) The following are also relevant: Common Law Human Rights Act 1998 Equality Act 2010 Protection Of Freedoms Act 2012 Freedom of Information Act 2000 Criminal Procedure and Investigations Act 1996

Step 3: CONSULTATION	
You should consider seeking the views of data subjects unless there is good reason not to. If the processing involves staff data, you should consider consulting them or their representatives. Consideration should also be given to consulting with Information Assurance (IA) for any new systems (that process personal data) and the audit capabilities within that system.	
3.1 Do you intend to consult with data subjects?	
☐ **Yes** Outline your plan in **Section 3.2** together with details of consultation with other stakeholders.	
☒ **No** Outline rationale[?].	The data being processed is for the primary purpose of conducting a criminal investigation; consulting with the data subjects will interfere with that investigation and therefore the course of justice. Members of the public, vehicles or identifying objects which are bystanders/not involved in the disorder could be captured on the

	footage however these objects will be blurred out and disregarded where required

3.2 Consultation Action Log
Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- Union representatives
- Information Assurance
- Legal
- OPCC
- PSD / Counter Corruption
- Partner agencies
- Data processors

Who	When	How	Outcome
Information Security	Scoping stage of project	Teams call	DPIA required (this) DPA required – competed 15.12.25 IA Baseline Security Document completed by Pimloc 13.10.25
Technology	Scoping stage of project	Teams call	Technical Information Security Questionnaire completed by Pimloc 13.10.25
Technology	Scoping stage of project	Request put in for Solution Architect	SA allocated for January 2025 – …
Finance	Grant application	Grant application completed and sent to HO	Grant confirmed Dec 2025
Procurement	Scoping stage of project	Agreed framework to use for the funded trial	DPA requested (with IA for approval 15/12/25)
Business Areas	Scoping stage of project	Ascertain business requirements, show a demo. Explain baseline requirements and that we have demo case files to use for the baselining	Ongoing

Step 4: ASSESSING NECESSITY AND PROPORTIONALITY

In this section you must demonstrate why the processing is necessary[?] and proportionate[?], providing evidence to support your assessment.

4.1 How will processing the personal data help to achieve your purpose?
Clearly state your objective and provide evidence for why the proposal is necessary. The evidence can consist of facts, statistics, reports etc.

It will provide a fast automated redaction solution to an otherwise labour intensive manual piece of work. Subject Access requests for example will be able to have the video element produced in a much quicker timescale and with less resource intensity.

4.2 Ensuring data minimisation

- Describe whether any less intrusive options would achieve the same goal.

- Could existing processes or techniques be used instead of new intrusive measures?
- Clearly outline why the processing is proportionate.

Existing practices that analyse and redact digital evidence require individuals to operate multiple disconnected systems, one at a time and in real time.
This relies on Investigators to use pieces of evidence they have discovered in various submissions and manually collate this together to track or redact. This is a time intensive and manual error prone process, in which Achieving Best Evidence (ABE) needs to be applied to keep a high level of data integrity.

4.3 Lawful basis

To process personal data you must have a lawful basis. Please select a lawful basis from the drop down lists (where appropriate). Guidance on lawful processing can be located on the ICO website.

Lawful Basis for Law Enforcement Data[?] *(If applicable)*: Necessary for a law enforcement purpose
Lawful Basis for General Data[?] *(If applicable)*: **Choose an item**

4.3.1 Lawful basis for special category data

If any of the special categories of data are being processed, you need to specify an additional lawful basis for processing this data. Please complete the section relevant to your proposal.

Law Enforcement Data[?] *(If applicable)***:**
It is based on law (please tick to confirm) ☒ ***Common Law Policing Purpose***
And
It is necessary for one of the following conditions (select from the list): Justice

General Data[?] *(If applicable)***:**
It is necessary for one of the following conditions (select from the list): Choose an item.
Or
It is in the substantial public interest and for the following purpose: Administration of justice

4.4 Describing compliance

You should include relevant details of how you will ensure compliance:

Data quality How do you intend to ensure and maintain good data quality?	Footage is already existing, this process will involve a human check for quality and accuracy
Transparency How do you intend to provide privacy information to people?	As per current NWP public privacy policy which outlines how NWP will process personal information for any footage received
Data subject rights What mechanisms will you put in place to ensure data can be searched, extracted, printed, deleted, rectified or restricted?	As per current procedure for any footage received Data will only be stored on the Pimloc system for 60 days as per NWP data retention agreement. Where a requirement to search, delete or rectify the data within the 60 days, all this capability is available within the Pimloc system. As per planned process, redacted copy will be uploaded to NiCE and available there for retention period in line with NPCC retention schedule
Processors If you are using a data processor, what measures do you take to ensure processor compliance? E.g. a contract, audit, sufficient guarantees.	…

International transfers Outline how you will safeguard any international transfers.	N/A
Purpose limitation How will you prevent function creep?	The software will only be made available to users trained in its use and whose role requires it. This will be managed by having an Azure group set up for user access to ensure no access possible if not included in the group.

What to do next

You will need to detail all data protection risks within steps 5 and 6 (on the following pages), including the impact on individuals (and their privacy) as well as risks to the organisation. To assist, these sections focus on specific data protection principles and privacy concerns. The risk matrix at the end of the document also provides support in determining the risk rating.

Step 5: RISK ASSESSMENT

Identify and assess risks

- ✓ Detail **all** data protection risks, privacy and the rights and freedoms of individuals.
- ✓ Consider the impact[?] on individuals and any harm or damage that might be caused.
- ✓ Where risks are identified, you must take steps to integrate solutions into the project and this must be recorded.
- **?** Examples of risk factors are provided as a starting point. You must ensure that all factors relevant to your proposal are considered. If you run out of space then insert my lines into the table. If you are unable to identify a risk then please state "**No risks identified**".

Risks to individuals include:	**Corporate risks include:**	**Mitigation/solution examples:**
• Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights	• Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations	• Deciding not to collect certain types of data • Reducing the scope of processing • Reducing retention periods • Taking additional technical security measures • Providing staff with training and guidance to understand the risks • Anonymising or pseudonymising the data • Using different technology • …

5.1 Being fair and lawful

Data must be processed lawfully, fairly and in a transparent manner[?]

- Have you identified the lawful basis of the project?
- Do you need to create or amend a privacy notice?

The data processed in Secure Redact is "Lawful", from the lawful basis that the data was seized; for example: Part 2 of the Police and Criminal Evidence Act 1984, Section 20, Extension of powers of seizure to computerised information. Investigatory Powers Act (2016) (IPA) brings together all of the powers already available to law enforcement to obtain communications and data about communications.

Data cannot be processed in Secure Redact without a reference that identifies the lawful purpose for which that data is being processed.

All data in Secure Redact is processed "Fairly", as: the data processing is purely factual, it is not modified in any way, nor it is (or can it be) unexpected or misleading.

The processing of sensitive data is Secure Redact is fair, lawful and strictly necessary as per the conditions identified below from Schedule 8, DPA2018

- Reasons of substantial public interest, specifically
    - The Administration of justice, such as the application of the Criminal Procedure and Investigations Act 1996, and
    - Preventing or detecting unlawful acts; such as (but not limited to) Rape and Serious Sexual Offences (RASSO)
- To protect the vital interests of the data subject or another individual; specifically, a victim of escalating crime leading to death.
- For the safeguarding of children and of individuals at risk; where the victim (or target) of crime is under the age of 18.

If the data being processed is not fair and lawful, it cannot be processed in Secure Redact

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**
	Remote Possible Probable	*Minimal Some Serious*	*High Medium Low*	*Describe the mitigation and whether it will be implemented*	*Is the risk: Eliminated Reduced Accepted*	*High Medium Low*
Discrimination	Remote	Minimal Impact	Low	The system will give uses potential matches to be used for intel purposes	Eliminated	Low
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.2 Having a specific, explicit and legitimate purpose

The purpose for processing personal data must be specified, explicit and legitimate, and not further processed in a manner that is incompatible with the original purpose for which it was collected.

- Does your project plan cover all of the purposes for processing personal data?
- Are all elements of the processing compatible with the original reason and justification for the processing?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.3 Recording adequate, relevant data and not being excessive

Personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed

- Is the quality of the information adequate for the purposes it is used?
- Are measures in place to ensure that data is limited to that which is needed to fulfill the aim of the processing?
- Which personal data could you not use, without compromising the needs of the project?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
The data will be stored in the forces DEMS system after processing	Remote	Minimal Impact	Low	The usage policy for the redaction solution will include explicit instructions to ensure the deletion of the downloaded footage both pre and post redaction is removed from the users one drive once the redacted version is uploaded to NiCE. This will be a temporary solution until Pimloc and NiCE implement the API which will remove the need for manual download and upload of the files.	Reduced	Low
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.4 Ensuring data is accurate & timely

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.

- If you are procuring new software, does it have controls in place to assist accurate data recording?
- Does the new software allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- Do you have processes in place to keep data up to date?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.5 Retention of personal data

Personal data must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data.

- What are the risks associated with how long data is retained and how they might be mitigated?
- Has a review, retention and disposal (RRD) policy been established?
- You may wish to consult the Force Records Manager.

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
Information could be stored in the system for longer than is required.	Possible	Some Impact	Low	There is a 60 day policy with Pimloc to delete all data over 60 days to eliminate duplication of data impacting any NPCC	Reduced	Low

				retention schedule requirements. In addition, the usage policy for the redaction solution will include explicit instructions to ensure the deletion of the downloaded footage both pre and post redaction is removed from the users one drive once the redacted version is uploaded to NiCE. This means NiCE remains the sole repository for the storage of the data and NPCC retention schedule requirements will be managed though that process. (API when complete will remove any risk of copies being downloaded to local storage)		
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.6 Keeping personal data secure

Personal data must be processed in a manner that ensures appropriate security[?] of the personal data, using appropriate technical or organisational measures.

- What technical and organisational measures are in place to ensure that the date is protected to an adequate level?
- What training on data protection and/or information sharing has been undertaken by relevant staff?

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk

Risk of unauthorised access to data, risk of data loss/corruption.	Possible	Some Impact	Low	Data being redacted will always be a copy of the original file. Pimloc Secure Redact does have an audit trail for each file redacted. In addition the original will always be available on NiCE should any concerns arise.	Eliminated	Low
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.7 Complying with data protection rights

Data Protection legislation gives data subjects various rights. Limiting or restricting any of these rights is likely to be a significant impact so the justification for any restriction, as well as mitigations, must be fully outlined.

- Consider each of the rights listed below and assess whether data subjects would be able to fully exercise these rights.
- For example: If an individual makes a Subject Access request, will you be able to easily identify, retrieve and extract the data to provide to the Information Assurance /Subject Access team?

Right to fair processing information[?]
Right of access (subject access)[?]
Right to rectification[?]
Right to erase or restrict processing[?]
Rights regarding automated decision making and profiling[?]
Right to object[?]

Describe the source of risk and the nature of potential impact on individuals[?] **and the organisation**[?]**.**	**Likelihood of harm**	**Severity of impact**	**Initial risk**[?]	**Mitigation/solution**	**Result**	**Residual risk**
N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.8 External data sharing and international transfers

Your processing may involve the sharing of personal data with 3rd party individuals, organisations or agencies.

- What contracts, information sharing agreements or memorandums of understanding are in place?

- What assessments have been made of the 3rd parties to ensure adequate provisions for the technical and organisational security of personal data?
- Has the organisation specifically asked suppliers to undertake a DPIA?
- If you will be making transfers, how will you ensure that the data is adequately protected? (especially if outside of the EU)
- …

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	Likelihood of harm	Severity of impact	Initial risk[?]	Mitigation/solution	Result	Residual risk
As per Pimloc Privacy policy - in the event that Pimloc undergoes a reorganisation or is sold to a third party, any personal information Pimloc holds about NWP may be transferred to that reorganised entity or third party. However none of NWPs personal information will be transferred to a third party prior to a sale or reorganisation completing.	Possible	Some Impact	Low	In built retention schedule within system limits video data to 60 days only. Privacy policy indicates NWP will be made aware prior to any change in 3rd party sale meaning use of service can be terminated if required.	Eliminated	Low
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.9 Human rights considerations

The European Convention on Human Rights sets out numerous rights and freedoms. Limiting or restricting any of these rights is likely to be a significant impact and result in a residual high risk. The justification for any restriction, as well as mitigations, must be fully outlined.

- If your actions will interfere with any of the rights listed below then you must clearly outline why it is necessary and proportionate.
- You must first consider: **Article 8: Right to privacy** – Will the proposal adversely impact an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications?

The Rights are:

Article 2: Right to life
Article 3: Prohibition of torture
Article 4: Prohibition of slavery or forced labour
Article 5: Right to liberty and security
Article 6: Right to a fair trial
Article 7: Right to no punishment without law
Article 8: Right to respect for private and family life without law
Article 9: Right to freedom of thought, conscience & religion
Article 10: Right to free expression
Article 11: Right to freedom of assembly and association
Article 12: Right to marry
Article 14: Right to freedom from discrimination

Describe the source of risk and the nature of potential impact on individuals? and the organisation?.	**Likelihood of harm**	**Severity of impact**	**Initial risk?**	**Mitigation/solution**	**Result**	**Residual risk**
N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

5.10 Additional risk factors

Describe any further risks, ensuring that any risks not already identified are included.

Additional risks may for example include:

- Internal data sharing - With which parts of the organisation is the information shared, what information is shared and for what purpose?
- If you are processing special categories of data then what risks have you identified?

Describe the source of risk and the nature of potential impact on individuals? and the organisation?.	**Likelihood of harm**	**Severity of impact**	**Initial risk?**	**Mitigation/solution**	**Result**	**Residual risk**
N/A	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

Step 6: LAW ENFORCEMENT RISKS

This section is only applicable to proposals involving law enforcement data. **Move to Section 7 if solely processing general data.**

6.1 Data logging requirements

Where data is processed electronically then logs must be kept for certain actions. This is to enable effective audit of processing systems, data sharing, and to verify ongoing lawfulness of processing.

- If the data is processed electronically, will a log be retained of the following actions?

• **Collection** • **Disclosure** • **Erasure** • **Alteration** • **Combination** • **Consultation**	☒ **Yes** ☐ **No (risk must be recorded)**

Describe the source of risk and the nature of potential impact on individuals[?] and the organisation[?].	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

6.2 Data categorisation requirements

When processing data for law enforcement purposes, you must provide where relevant and as far as possible a clear distinction between categories of data subject.

- Will there be a clear distinction between different categories of personal data subjects, for example subjects who are:

• **Suspected of having committed, or are about to commit, a criminal offence** • **Convicted of a criminal offence,** • **Victims of a criminal offence,** • **Witnesses to a criminal offence.**	☒ **Yes** ☐ **No (risk must be recorded)**

Describe the source of risk and the nature of potential impact on	**Likelihood of harm**	**Severity of impact**	**Initial risk[?]**	**Mitigation/solution**	**Result**	**Residual risk**

individuals[?] and the organisation[?].						
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

In Step 7, please indicate where mitigation/solutions and residual risks have been approved by the Head of Department/Information Asset Owner.

Step 7: OUTCOME AND REVIEW		
Item	**Name/Date**	**Notes**
Solutions approved by:		Integrate actions back into the project plan, with date and responsibility for completion.
Residual risks approved by[?]:		The Head of Department/Information Asset Owner must approve all residual risks.
If any residual risks remain High		
Date forwarded to DPO:		If any residual risks remain High, please forward initially to the Data Protection Officer (DPO) for their advice.
Summary of DPO advice: Click here to enter text.		
Date forwarded to CIO/SIRO:		Any residual risks remaining High must be referred to Chief Information Officer (CIO)/Senior Information Risk Officer (SIRO) for the risk to be accepted prior to referral to ICO.
High risk(s) accepted by:	Name: SIRO/CIO *(please delete as appropriate)* Date:	
Date forward to ICO		If accepting any residual high risk, the ICO must also be consulted before commencing processing.
Review		
A DPIA is a process that should be reviewed throughout the lifecycle of the processing – it does not end at go live.		
Please outline the review process that you will undertake to ensure that the risk mitigations have been successful and that no new risk factors have emerged. Please also include; • who will be responsible for reviewing the processing; • the frequency of the review; and • the date of the next review.		

DPIA Nov 2018 (V 1.0)

DPIA DPIA (v1.0)
OFFICIAL
(Update when complete)

This will be reviewed throughout the initial funded trial with any issues being addressed. A full review of the DPIA will happen if the solution proves successful and we look to move forward with the software.

How to identify and assess risks (Risk Matrix) *(Click the triangle to expand)*

You will need to consider the potential impact on individuals and any harm or damage that might be caused by the processing – whether physical, emotional or material. In particular, look at whether the processing could possibly contribute to:

- Inability to access rights or access service or opportunities;
- Loss of control over the use of personal data;
- Discrimination;
- Identity theft, fraud or financial loss;
- Reputational damage;
- Physical harm;
- Loss of confidentiality;
- Re-identification of pseudonymised data; or
- Any other significant economic or social disadvantage.

You will also need to include an assessment of the security risks and the potential impact of a breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is high, you will need to make an 'objective assessment' considering both the likelihood of harm and severity of impact. The matrix below assists to determine the initial risk.

Risk Matrix:

DPIA Nov 2018 (V 1.0)

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some Impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Possible	Probable
		Likelihood of harm		

DPIA Nov 2018 (V 1.0)