DPIA Screening Checklist

If you intend to process any types of the personal data set out in List 1 and the processing appears in List 2 a DPIA must be conducted.

List 1 **Types of Personal Data processed**	List 2 **Types of high-risk Processing**
Racial or ethnic origin	Innovative use or new technology or solutions
Political opinions	Denial of service or rights
Religious or philosophical beliefs	Large-scale profiling, evaluation or scoring
Trade union membership	Biometrics or genetic data
Genetic data	Automated decision-making
Biometric data	Combining or matching datasets
Health data	Invisible processing
Sex life	Tracking or monitoring
Sexual orientation	Targeting of children or other vulnerable individuals
Criminal activity	Risk of physical or mental harm
Allegations	
Investigations	
Proceedings	

Confirm which (if any) of the above apply:

The personal data held within the PND will be checked to establish if there are any allegations, investigations or ongoing proceedings that relate to serving police officer, police staff, special constables, and volunteers, so that an assessment can be made by individual forces as to the impact of such report(s) upon the role and function conducted by the individual in their organization.

The relevant types of personal data and high-risk processing in the table above have been indicated through the use of underlines.

Data Protection Impact Assessment (DPIA) – Stage 1

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to refer to the guidance material available before completing the form.

Data Protection Impact Assessment (DPIA)			
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.			
Section 1 - Governance			
Project Proposal Name:		Home Office Data Wash	
Information Asset Owner:		Police and Crime Commissioner	
Information Custodian:			
DPIA Coordinator:		DPO – Andrea Gabbitas	
Date on which processing will commence:		April 2023	
Date submitted to DPO:		May 2023	
Note: DPO will give an **initial response** within 10 working days of receiving the completed form.			
DPO Assessment			
<u>DPO Use Only</u>			
A. DPIA is not mandatory.	☒	This part I is sufficient	
B. DPIA is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA will be required.	☐		
C. DPIA is mandatory.	☐		

Section 2 - Purpose, Scope and Context

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

In recent years there has been a continued decline of public confidence in policing caused by numerous cases in which police offenders have committed serious offences. Whilst the impact of the actual offence(s) cannot be underestimated, there have been occasions in which relevant information was held within the PND prior to the offending and therefore potentially missed opportunities for intervention or prevention.

Op Fairstay, also called the Home Office Data Wash is a requirement for all police forces, and optional for all Police and Crime Commissioners, to submit HR data to the centre so that it can be washed against PND. This is in an effort to proactively identify any potential concerns regarding integrity and identify any unknown criminal or otherwise incompatible behaviour of officers and staff. The integrity testing of personnel using our own data in order to better deter, identify and deal with those whose conduct falls below the standards required to maintain public trust and confidence, and our legitimacy with the public underpins the reason for the data wash.

There is a DPIA produced by the HO for the initial data collection from forces, the wash itself and the return to forces.

2.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

Names, DOB, addresses, criminal records.

2.3 Will special category data be used in the proposal? (Select all that apply)

☐ Race	☐ Trade union membership
☐ Ethnic origin	☐ Genetic Data
☐ Political opinions	☐ Biometric Data
☒ Sex life	☐ Sexual orientation
☐ Religion	☐ Health
☒ Philosophical beliefs	☐ None
	Only as these categories may appear within a crime report. EG – if there's an arrest for lewd behaviour that could be categorised as sex life.

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in the WMP's possession, from a different force.

It is anticipated forces will be their own data controller for the purposes of the HDW. Where a local decision is made to include Police and Crime Commissioner personnel in the HDW the PCC is likely to be a controller of their staff data.

The data held within the PND is within a restricted system to which only appropriately vetted, trained and authorised people are able to gain access. The completion of the HDW will take place within a secure technological environment with organisational measures to protect personal data. These measures are already accredited to the Home Office standards required for the PND accreditation. Of all the processing operations, the actual checking of the HDW results and associated research is perhaps the activity where any loss of confidentiality would be the most damaging.

This is different as the force is receiving the results of the data wash in one (or several) large documents (spreadsheets?).

2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

Where an individual officer or staff has had a "hit" on the PND wash, vetting staff in PSD will carry out further Intel and systems checks. The results will be compared to NPCC vetting standards to understand if they are potentially incompatible with working for the OPCC either at all, or in certain higher vetted positions.

Those individuals that cause concern will be contacted and further discussions will take place. Various outcomes are possible – none, manager made aware and risk mitigation in place, individual moved role, disciplinary or criminal investigation.

2.6 How many individuals 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

2.7 What categories of data subject are 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

☐ Children or vulnerable individuals

☒ WMP staff (current and former)

☐ Other

If other then please provide further details below:

Click here to enter text.

2.8 Will it involve the collection of new information about individuals? Will WMP collect data that it has not previously collected or had access to?

☒ Yes

☐ No WMP had access to PND.

2.9 Data Sharing **Does the processing involve:**		**Select one option**
2.9.1	Data being shared with third parties external to WMP or recipients that have not previously had routine access to the information?	☐ Yes ☒ No Not this part.
2.9.2	Transferring data outside the UK but within the EU?	☐ Yes ☒ No
2.9.3	Transferring data outside the EU?	☐ Yes ☒ No
2.9.4	Storing data using a cloud service provider?	☐ Yes ☒ No
2.9.5	Is there an ISA, contract, or other sharing agreement in place with all parties with whom data will be shared?	☐ Yes – agreements in place ☐ Not yet – agreements required ☒ No – none required

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?
For example, can the aim be achieved by using less data or different types of data?
Are all categories of data necessary to achieve the aim?

There is no possible way to undertake the data wash without using their personal information to identify them.

The quality and accuracy of the information provided will impact upon the number of search results forces subsequently received for review. The previous learning from delivering two HDWs is that

this information is more readily available and accurate from existing HR systems than vetting records as they are more often updated by staff, but this will be an individual forces decision as to which system(s) are used to complete the submission.

The PND includes records relating to individuals that police forces obtain during their lawful operational function and record the personal data for which there is a policing purpose. The PND is loaded with personal data owned by forces which are in the groupings of crimes, intelligence, custody, child abuse and domestic abuse investigation, and so the PND's criteria is predefined and outside of this DPIA's scope.

2.11 Explain how the use of personal data is proportionate to the aim of the proposal.
Weigh the advantages of achieving your purpose against disadvantages to data subjects.

Recent cases involving corrupt police officers have caused national concern. Public confidence is very low and the data wash is proportionate in order to address that. The HO has enforced the national data washing process. There is substantial public interest in the work. The data wash is essential to ensure the public can have full confidence in the staff who work for the PCC.

In recent years there has been a continued decline of public confidence in policing caused by numerous cases in which police offenders have committed serious offences. Whilst the impact of the actual offence(s) cannot be underestimated, there have been occasions in which relevant information was held within the PND prior to the offending and therefore potentially missed opportunities for intervention or prevention.

Section 3 – Lawful Basis

3.1 Lawful Basis
To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.

The PCC needs to ensure public confidence. The integrity testing of OPCC staff using our own police data in order to better deter, identify and deal with those whose conduct falls below the standards required to maintain public trust and confidence, and our legitimacy with the public underpins the reason for the need to conduct a HDW.

The HDW processing activity will be predominantly for General Purposes but in some cases could be regarded as moving to Law Enforcement Purposes should a 'trace' identify criminal behaviour.

3.2 Further Special Category Lawful Basis
If processing special category data (section 2.3) you must have identified a further lawful condition

One of the following conditions applies (select from the list):
Choose an item.

Data:
It is necessary for one of the following conditions (select from the list):

Employment **OR** It is in the substantial public interest (tick to confirm) ☒ **AND** for the following purpose: Statutory function

Section 4 – Review, Retention and Disposal
4.1 Does the proposal have a review, retention and disposal process that complies with OPCC Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within the WMP IM document suite.
☒ Yes (the standard retention and disposal process for HR documentation will be applied) ☐ No

Section 5 – ICO: Additional Factors

The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.

Does the processing involve:		Please check either Yes or No	If 'Yes' then please provide further details
5.1	**Systematic, extensive and large scale profiling and automated decision-making about people?** *"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"* Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an individual, including the analysis or prediction of an individual's performance. Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.	☐ Yes ☒ No	Human intervention is involved before any decisions or further action. Once PSD has completed the data wash, decision making will only be undertaken with senior management within the OPCC and consultation with the DPO.
5.2	**Large scale use of special category data or criminal offence data?** *"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"*	☒ Yes ☐ No	The results are all about people who have had some police contact.
5.3	**Public monitoring?** *"Systematic monitoring of a publicly accessible area on a large scale"*	☐ Yes ☒ No	
5.4	**New technologies or techniques?**	☐ Yes ☒ No	

	"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"		
5.5	**Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?** *"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"*	☐ Yes ☒ No	
5.6	**Biometrics/genetic data?** *"Any processing of biometric data"* **and/or** *"any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject"* Biometric data can include Facial Recognition technology, fingerprints and is defined as	☐ Yes ☒ No	
5.7	**Data matching?** *"Combining, comparing or matching personal data obtained from multiple sources"*	☐ Yes ☒ No	
5.8	**Invisible processing?** *"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"* For example, when gathering data, without the knowledge of the data subject, in the course of a Police investigation.	☒ Yes ☐ No	This is a national initiative involving such a large number of people that individuals have not been personally contacted as it would be disproportionate to do so. However, due to the nature of our role, staff regularly complete and submit ne vetting information and staff were informed that the exercise was taking place.
5.9	**Tracking?** *"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"*	☐ Yes ☒ No	
5.10	**Targeting of children or other vulnerable individuals?**	☐ Yes ☒ No	

	"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children For example, the use of personal data relating to children for the purposes of marketing their online safety products.		
5.11	**Risk of physical harm?** *"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals".* For example, if data relating to CSAE, HUMINT or protected persons data was compromised then it could jeopardise the safety of individuals.	☐ Yes ☒ No	
5.12	**Evaluation or scoring?** *"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of a recruitment process.*	☒ Yes ☐ No	Evaluation of suitability for post.
5.13	**Data processed on a large scale.** *Considerations include:* • *The number of data subjects concerned* • *Volume of data and/or range of data items* • *Duration, or permanence, of the data processing* • *Geographical extent of data processing*	☐ Yes ☒ No	In the region of 100 staff involved, and therefore this may not be large scale however we understand this is all members of our staff.
5.14	**Preventing data subjects from exercising a right?** *The rights are:* • *The right to be informed* • *The right to access data* • *The right to rectification* • *The right to erasure* • *The right to restrict processing* • *The right to object* • *The right to portability* • *Rights relating to automated processing*	☐ Yes ☒ No	

Please forward the completed form to the OPCC DPO.