Data Protection Impact Assessment (DPIA) Screening Checklist & Template

Historical Data Wash of police officers, police staff, special constables and volunteers using the Police National Database (PND).

Preamble

The NPCC, as a Controller, is required to comply with Data Protection legislation – (i) the Data Protection Act 2018 (DPA) when it processes personal data for any of the Law Enforcement Purposes, and (ii) the UK GDPR, as supplemented by the DPA, when the processing is for General Purposes (anything that does not fall under the Law Enforcement Purposes definition).

One of the obligations arising from the Data Protection legislation is the requirement for the NPCC to conduct a Data Protection Impact Assessment (DPIA) where the prospective processing of personal data is likely to result in a '**high risk to the rights and freedoms of individuals**'.

Even if that 'high risk' threshold is not reached, the NPCC's position is that it is good practice to complete a DPIA, particularly when developing a Data Sharing Agreement.

The DPIA must be undertaken prior to the processing starting and, in some cases, cannot commence without the prior authorisation from the Information Commissioner's Office (ICO) once they have reviewed the DPIA

The relevant parts of the Data Protection legislation concerning DPIAs can be found at:

- Section 64 of the DPA and Section 65 of the DPA for processing for Law Enforcement Purposes; and,
- Article 35 of the UK GDPR and Article 36 of the UK GDPR for processing for General Purposes.

The ICO has produced extensive guidance on DPIAs for processing for Law Enforcement Purposes and General Processes.

Screening

In order to determine whether a DPIA is required it is necessary to first conduct a screening exercise to assess whether the prospective processing of personal data is likely to result in a 'high risk to the rights and freedoms of individuals.

The screening should occur where there is any new or significant changes to existing processing of personal data.

Even if the screening does not result in a requirement to conduct a DPIA it is often beneficial to conduct one.

A DPIA Screening Checklist appears on the next page which should be used to determine if a DPIA is required.

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.

Screening undertaken by: **Allan Harder – Police Crime Prevention Initiatives. (Police CPI).**

Date undertaken: 1st February 2023.

Outcome of Screening:

The outcome of the screening check list is that a DPIA is required and a DPIA will be completed so that the Historical Data wash of police officers, police staff, special constables and volunteers using the Police National Database (PND) can be completed.

If the Screening Checklist identifies a requirement to undertake a DPIA (or you choose to undertake one) please move on to the next page. If there is no requirement, please email this document with the fields above completed to dpo@npcc.police.uk

NPCC DPIA Template

The template, starting on the next page, has been derived from the ICO's and can be completed to record details of the DPIA process and outcome.

Steps 1 to 5 and parts of 7 should be completed by an appropriate person with the necessary knowledge of the processing of personal data being considered (normally the Business Subject Matter Expert (SME) and/or Business Lead[1]).

The NPCC DPO will assist completion of the template where required and in any case will complete Step 6 and parts of Step 7.

The fields requiring completion can readily be identified through appearing with a pale blue/green background when a cursor is hovered over them.

[1] Business Lead is likely to be the Portfolio Lead or Head of National Unit. Subordinates with necessary knowledge and authorisation can participate in the completion of this document

Data Protection Impact Assessment (DPIA)

Historical Data Wash of police officers, police staff, special constables and volunteers using the Police National Database (PND).

Freedom of Information Act & Information Security

This document (including attachments and appendices) may be subject to an FOI request and the NPCC FOI Officer & Decision Maker will consult with the author on receipt of a request prior to any disclosure. For external Public Authorities in receipt of an FOI request concerning this document, please consult with npcc.foi.request@npfdu.police.uk.

In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this document is strictly on a need-to-know basis and in compliance with other security controls and legislative obligations.

Purpose

This DPIA document has been used to:

- identify any privacy or information risks concerning the processing of personal data
- determine any mitigations necessary to bring those risks down to an acceptable level
- provide a record of those mitigations and the decision by Business Lead whether to accept and adopt them
- provide a record of the NPCC's Data Protection Officer's views on the initiative.

Document Administration

Government Security Classification:	**OFFICIAL.**
If OFFICIAL-SENSITIVE set out any handling instructions below:	
For inclusion in FOI Publication Scheme?	**Yes.**
Version:	1.0
Author(s):	**Allan Harder - Police CPI.**
Date Issued:	**2nd February 2023.**
Date to be next reviewed:	**tbc**

Information Asset Owner (IAO) for this document: **Chair NPCC Prevention Coordination Committee.**

Leads' Details

NPCC Coordination Committee overseeing initiative:

NPCC Prevention Coordination Committee.

NPCC Portfolio overseeing initiative:

Police CPI.

National Unit overseeing initiative:

NPCC

Business Lead for initiative:

CC Kennedy.

Information Asset Owner(s) for information involved in this initiative:

Multiple as identified by individual Police Forces.

Business SME(s) involved in creation of this DPIA:

Allan Harder – Police CPI.

Data Protection Advisor:

Andy Begent, NPCC Data Protection Officer.

Comments:

This DPIA provides a generic assessment of information risks and necessary mitigations applicable to all police forces in relation to the Historical Data Wash.

All police forces should review the contents and document supplementary or alternative DPIAs to address their individual circumstances.

Step 1: Introduction

This section is intended to provide a concise introduction to the initiative, how it arose and the processing of personal data it involves.

1a. Provide a short introductory summary of the intended processing, including the purpose(s) of the processing and the desired outcome of the processing.

The Historical Data Wash (HDW) is a defined activity within a period of time, 27th January 2023 to 29th September 2023.

The HDW will use the names, dates of birth and addresses of all police officers, police staff, special constable and volunteers to complete a search of the Police National Database (PND) to proactively identify any potential concerns regarding their integrity.

Where concerns are identified the necessary interventions will be made by the respective police forces concerned and such activity falls outside the scope of this DPIA.

1b. Describe where the intention for the processing arose from i.e. who decided to progress this initiative, in response to what?

In 2021, North Yorkshire Police and partner agencies implemented Project Shield, which successfully used information in the Police National Database (PND) with the intention of improving the multi-agency response to safeguarding victim of domestic abuse who had protective non-molestation orders against alleged perpetrators.

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.

Since December 2021 Police CPI and CGI, with the authority from CC Martin Hewitt, Chair of the NPCC have worked together to explore options for using the PND and its data set to support police activity in respect of the screening of police employees to improve the integrity levels of the police service and improve public confidence.

This engagement resulted in Project Prism conducted within North Yorkshire Police where the concept was proven, and the benefits evidenced.

Under the direction of Chief Constable Serena Kennedy, NPCC Strategic lead for Prevention, there has been development of the projects learning towards a national program. This has included a Historical Data Wash (HDW) initiative with the Metropolitan Police Service, Operation Trawl which confirmed the learning is scalable for future delivery to the 300,000 police officers, police staff, special constables and volunteers involved in UK policing.

The integrity testing of police personnel 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.

1c. Confirm whether the processing is for Law Enforcement Purposes or General Purposes. (within policing if the processing is not for Law Enforcement Purposes it will be for General Purposes). Processing could be for both Law Enforcement and General Purposes.

Both Law Enforcement Purposes and General Purposes. The HDW processing activity will be for General Purposes but in some cases could move to Law Enforcement Purposes should a 'trace' identify criminal behaviour.

1d. If relevant, describe what non-Data Protection legislative framework supports or requires the processing i.e. is the processing mandated or required by an Act of Parliament?

Common Law Policing purposes.

Step 2: Describe the processing

This section is intended to provide details of the personal data involved and how it will be processed throughout its lifecycle.

Processing Operations

2a. Describe how the personal data involved will be obtained or created, including from where, by whom, by what means, when, and how frequently.

The HDW involves the comparison of two data sets namely the PND and a force record of its staff.

CGI are a private sector IT services and consulting company that designed, built, delivered, and maintain the Police National Database (PND) on behalf of the Home Office and UK Policing and their partner agencies. CGI's contractual obligations are driven by the Home Office engagement and police business development and ideas for change are managed through engagement with the NPCC lead for PND.

PND comprises crime reports, custody records, intelligence reports, child abuse and domestic abuse investigations created by all UK police forces as part of their operational daily activities. These five groups of reports are subsequently copied onto the PND by automated and semi-automated data feeds and made available to all police forces via the PND.

The PND is updated as and when the force data is amended or deleted, and such updates occur daily.

The second data set will be created by the 10th February 2023, there is a need for all forces to provide the names, dates of birth and addresses of all police officers, police staff, special constables and police volunteers for the purposes of the HDW, irrespective of rank and roles.

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 provision of an occupancy date for addresses, if recoverable, significantly reduces the search results being received and the need for future research.

A formatted collection template (excel spreadsheet) has been shared with all forces so that the data received is in the correct format and structure, ensuring an effective search of the PND.

A formatted HDW results templated will be populated by CGI and returned to individual forces using the secure file transfer protocol. The formatting of the HDW results provides performance data within the agreed NPCC measures using non personal statistical data. Police CPI will engage with each force at agreed intervals to obtain the details of the performance data so that national reporting to the NPCC can be delivered centrally.

It is a force decision as to who completes the personal data extraction, but this will only be completed once and within the scope of the NPCC HDW request.

It is recognised that new information relevant to the HDWs purpose will be added after the check is completed. It is appropriate.

2b. Once the personal data has been obtained set out in chronological order and stage-by-stage how it will be subsequently processed. For each stage describe the processing operation involved,

including what will occur, who will be involved, when and how frequently it will occur. Processing will include storage, amendment, disclosure, sharing and disposal of the personal data.

The processing of personal data relating to Police officers, police staff, special constables and volunteers through the PND is compliant with the College of Policing APP for Vetting.

Significant dialogue has been held with key NPCC portfolio leads including PND, Counter Corruption, Professional Standards, DEI, Workforce and NPCC Legal, FOI and Comms Teams achieving national support in response of the Home Secretary's statement this will be completed.

The processing will involve individual police forces as the data controllers providing data from their HR and or vetting records which consists of names, dates of birth and current home addresses for persons within the above groups.

Collectively across the UK this is estimated to be 300,000 people.

By Friday 10th February 2023, each force will send a password protected data file that details the names, dates of birth and addresses of their Police officers, police staff, special constables and volunteers via secure file transfer protocol to CGI, the data processor, who deliver the PND on behalf of UK policing.

By Friday 31st March 2023, CGI as the data processor will conduct a series of searches using the provided details to complete a Historical Data Wash of the data files provided by forces against the 5.6 billion searchable records held within the PND without creating nominal records in the system.

The protections already in place under the existing PND contract mean that CGI can store, copy, disclose, or use the Authority Data only as necessary for the performance of our obligations.

CGI will complete the Historical Data Wash for all the individual forces removing any duplicate results for individual before sending the returns to the respective force. At this point of return the processing aspect of the HDW ceases.

From the 31st March to 29th September 2023, forces will manually review the HDW results to establish if the reported HDW returns relate to a member of their force. When the results do relate to a member of the force further work is needed to establish if the information had been previously disclosed and if such a disclosure was required.

If there is new information that required disclosure to the force, it will be assessed by the police force and decisions made regarding any actions to be taken in accordance with relevant policies and College of Policing APP. These could involve dissemination of the information elsewhere in the police force, conducting an investigation leading to disciplinary action or criminal investigation, and potentially prosecution. These processes may result in the creation of additional information on force systems.

2c. Confirm whether any of the processing will involve joint controllership with another controller(s). If so, describe when and how the personal data becomes subject of joint controllership.

It is anticipated forces will be their own data controller for the purposes of the HDW.

There will be cases where joint controllership will occur where two or more police forces have a combined HR function involved with preparation of the data set for submission or where there is a combined function that would receive the HDW results.

In forces where there is joint controllership, there will be a need to consider and document a joint agreement.

2d. Confirm whether or not any of the processing will involve the use of a processor to process personal data on behalf of the NPCC. If so, describe when and how the personal data becomes subject of processing by a processor.

The HDW results received by forces from CGI will require review by an identified, authorised, and trained member of staff so that these are processed correctly.

2e. Describe the extent to which there is likely to be public, media or pressure group concerns over the processing.

The work completed in 2022 that proved the concept of using the PND to check the integrity of those working in policing was prompted by a high profile case. Since that time further high-profile cases have emerged attracting additional media interest, public concern, and comments from groups.

In response to these cases the use of the PND for this very purpose has been directed by the Home Secretary and reported in the national media without concern.

Staff associations are interested in the processing and engagement is taking place with them to provide reassurance that the HDW being completed is both lawful and proportionate.

2f. Identify which, if any, of the processing operations could potentially present high risks to the confidentiality of the personal data involved.

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.

Force HR systems will have accreditation required for the storage and management of personal data and internal policies are expected to prescribe these.

The extraction of the HR data set for the purposes of the HDW is into a spreadsheet format and towards reducing the risk of the personal data being compromised, advice has been given to all forces this is password protected.

The transfer of the HR data set to CGI for the HDW and the transmission of the results is via the Secure File Transfer Protocol, which is the method used for providing daily PND updates.

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.

2g. Describe the extent to which the processing will be novel, new, or not resembling processing previously occurring.

Police officers, police staff, special constables and volunteers are subject to vetting checks at various points in time such as recruitment and change of role, but the timing between these varies significantly. As a result, changes in a person's circumstance may not be evident or disclosed thereby causing organisational risk.

The novel aspect of the HDW is that it will apply to all at a moment in time, identify changes in circumstances that have not been disclosed reflecting upon the individual's integrity, and provide a national coordinated results to a common standard which can be reported.

2h. Provide an overview of the measures to be put in place to ensure adequate security/maintenance of confidentiality of the personal data when it is processed. These measures may be technical or organizational ones proportionate to the nature of the personal data involved. Technical measures can be defined as the measures and controls afforded to systems, devices, networks and hardware and encompass cybersecurity, encryption and pseudonymisation, physical security, secure disposal, passwords and access controls. Organizational measures may consist of

internal policies, organizational methods or standards, and controls and audits. They can include information security policies, business continuity plans, risk assessments, polices & procedures, awareness & training, reviews & audits, and due diligence.

There are already adequate measures in place created within individual forces and published APP by the College of Policing to maintain the confidentiality of personal data when it is processed. These will include the ability and completion of regular audits of systems to establish who accessed records at specific times and dates and the policing purpose.

The delivery of the NPCC HDW includes several stages and measures to ensure the effective delivery, which include:

- **Delivery of awareness events to identified force leads, and the provision of guidance documents in support of the HDW process and completion.**
- **The identification of trained and vetted staff to conduct the HDW activities.**
- **Providing HDW training to those conducting the results review work and their supervisors.**
- **Forces using a small and dedicated team to complete the review activity.**
- **Providing directions to forces that staff who conduct the HDW reviews do not complete these on people they know or work with.**
- Providing directions to forces that staff processing the data returns will be reminded of their duties, responsibilities and expectations regarding confidentiality and conduct with regard to the data returns.
- **The creation of two weekly review meetings with individual forces and the Police CPI delivery team.**

2i. If the processing involves use of new or altered software or IT infrastructure describe what measures have been put in place or are planned to ensure that software or IT infrastructure has or will be accredited to confirm it is suitable secure to use.

Current IT systems and software is being used for the HDW and will be subject to information assurance and accreditation within forces.

2j. Describe the processes that will ensure the personal data will not be retained longer than is necessary for the purposes set out at 1a.

Police forces will adopt measures to comply with College of Policing Authorised Professional Practice (APP) and the NPCC's National Guidance on the Retention and Disposal of Police Records Version 4, November 2020 concerning retention, review and disposal of information.

Subject to NPCC approval, CGI will retain the forces' data submission and the HDW results for 12 months. This permits time for unexpected questions on whether specific data or actions were completed, and therefore affords an opportunity to review the searches completed. These will be retained within a secure area of the PND which cannot be searched by users. If forces request that the data is deleted prior to the years that would be completed.

Nature of the Personal Data

2k. Describe the type personal data involved, including whether it is Criminal Offence Data[2], Special Category Data[3], or data subject to Sensitive Processing[4]. Where appropriate list data fields.

The data provided by forces for the purpose of the HDW comprises of a subset of the nominal details already in existence for police personnel obtained during recruitment and initial vetting processes. It will not contain any Criminal Offence Data, Special Category Data or data subject to Sensitive Processing.

The HDW results will contain trace PND Data and will therefore contain some Criminal Offence Data, Special Category Data or data subject to Sensitive Processing here. The full details of the PND data will not be included in the HDW returns as there is a requirement for the reviewer to access the PND to assess the report and its relevance.

2l. Describe the volume of personal data involved, including how many individuals it will relate to.

Research has been completed and this is supported by a request to all forces to provide their respective numbers of police officers, police staff, special constables, and volunteers.

This has identified almost 300,000 individuals within the UK.

The PND contains 5.6 billion searchable records relating to crimes, custody, intelligence, child abuse and domestic abuse investigations.

2m. Describe any criteria used to determine what personal data will be processed.

The criteria to determine if personal data will be processed as part of the HDW is simply "is the person a serving police officer, member of police staff, special constable or volunteer?".

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.

2n. Describe the measures to be put in place to ensure an excessive amount of personal data is not processed. These may be technical and/or organizational ones.

Upon deciding what personal data will be used, that answer is provided by the minimum search requirements needed to identify a trace within the PND, namely name, date of birth and address.

---

[2] Defined where processing is for General Purposes as personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

[3] Defined where processing is for General Purposes as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[4] Defined where processing is for Law Enforcement purposes as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, or of biometric data, for the purpose of uniquely identifying an individual; data concerning health an individual's sex life or sexual orientation.

2o. What measures will be put in place to ensure the personal data processed is of the necessary quality (accurate, complete, clear etc). These may be technical and/or organizational ones.

Forces currently hold personal data within their HR and vetting systems and consequently will have internal policy and procedures to ensure their quality is maintained. These policies are likely to include an element of personal responsibility from the individual to whom the personal data relates. It is from these records that personal data is being obtained for the purposes of the HDW.

Equally force records relating to five categories within the PND are collected and provided by them during operational and daily policing activities for which there are requirements for data quality and accuracy.

Data Subjects

2p. Describe the types/categories of the data subjects whose data will be processed e.g. victims. witnesses, offenders, suspects, officers, staff etc.

The data subjects who will be subject of the HDW are police officers, police staff, special constables, and volunteers irrespective of rank or role within policing.

The PND contains details of suspects, witnesses and victims.

2q. Confirm whether the personal data is processed based on data subjects' consent and if so, describe how that consent will be obtained and recorded, and how withdrawals of consent would be managed.

This is not applicable for the HDW. Consent is not used as a basis for processing and should not be confused with fairness.

Forces will inform their personnel that the HDW is taking place to be fair and as part of the aftercare requirements of force regarding vetting and employment, but do not need their consent to undertake the HDW as consent is not the legal basis this activity.

2r. Describe the extent to which the personal data involved will relate to children or other vulnerable people.

The force HR and vetting data will relate to individuals who fall with the groups of Police officers, police staff, special constable and volunteers and not specifically children. It is anticipated that very few people would be under 18 years of age and if so that would only be within the police staff and volunteer groups. A decision has been taken that police cadets will not be subject of the HDW and are excluded and would predominantly be children.

Vulnerable people may be within the groups of Police officers, police staff, special constable and volunteers and the performance measures to be agreed by the NPCC are intended to identify the extent to which the HDW impacts upon some of those who may be vulnerable.

The PND will include personal data relating to individuals who are children and vulnerable adults.

2s. Describe the nature of the NPCC's relationship with data subjects, including whether they would expect their personal data to be used in this way, and the extent to which they can influence the processing.

Police officers, police staff, special constable and volunteers are and have been subject of pre employment checks and or vetting, and therefore will be aware that a pre-requisite of vetting is the need to be periodically rechecked thereafter and that the PND would be used.

Some may be aware from their interactions with the police that their data is in the PND but due to the 5 PND categories others will not be aware.

Step 3: Consultation

This section is intended to stimulate consideration as to whether the views of internal or external stakeholders should be sought. Initiatives that have the potential to lead to public or media concern may benefit from consultation that could help enhance the processing. Clearly external consultation may be counter-productive if it were to reveal sensitive policing techniques or capabilities. Where the processing is largely consistent with a well-established approach there may be little benefit in consultation.

3a. Describe the extent to which you intend to consult, or already have consulted, with stakeholders on their views of the processing described in response to 2c. Stakeholders can include externally - data subjects, members of the public, campaign groups, partner organizations; internally – information security experts, ethics committees etc.

Consultation for the HDW and processing described in 2c has taken place within the NPCC Prevention Coordination Committee.

Key NPCC Portfolio Chief Leads have been consulted to ensure that there is join up including Vetting, PND, PSD, Workforce, EIA and Counter Corruption. In addition, the team will be consulting through the EIA Committee (7th February).

Police Staff associations and Trade Unions have been engaged and their view sought by the NPCC workforce lead.

Police CPI's executive board which consists of the Chair of the National Police Chiefs' Council in addition to 7 other chief constable members have been consulted.

As stake holders the Home Office have been informed of the HDW.

3b. If consultation is not intended or is to be limited set out a rationale for adopting that position.

Not applicable.

Steps 4 & 5: Identify risks, assess risks, and determine measures to reduce risks

The table overleaf sets out in Column 1 generic information risks that could apply to the processing of personal data under any initiative.

Columns 2 and 3 should be used to record the results of a risk assessment that should be carried out on each potential risk, the numerical result of which should then be added to Column 4.

Once the risk assessment has been conducted the Business Lead for the initiative covered by this DPIA should determine, against their risk appetite, whether the risk should lead to termination of the initiative, or alternatively can be tolerated, or transferred or treated. These terms are described below:

- Terminate - Some risks are so far beyond the tolerance identified by the risk appetite or are assessed as having such a severe impact on the business that the initiative should not be progressed.
- Tolerate – some risks are of a sufficiently low level that no actions need to be taken.
- Transfer – on rare occasions it could be possible to transfer the risk to third-parties.
- Treat – many risks can be treated or mitigated to reduce them to a level that is acceptable to the Business Lead.

Where the decision is to treat the risk the treatment to be applied should be added to Column 7 – Column 6 provides potential risk treatments which can be used as prompts for the completion of Column 7.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	5. Decision (Terminate, Tolerate, Transfer or Treat)	6. Potential Risk Treatment	7. Risk Treatment to be adopted, or comments
Confidentiality-related						
IR1. The information is accessible by people who should not have access to it	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Restrict access to the information through appropriate technical, physical or procedural means so that only those with a legitimate justification can access it Anonymise or pseudonymise the information where possible	**This can be mitigated by existing measures that restrict access to HR and Vetting Data, and the PND.** **Access to the HDW results will need to have limited access though appropriate technical, physical or procedural means so that only those with a legitimate justification can access it.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).** **Recommendation IR1-1: Access to Vetting Data, HDW results and PND is limited through technical and procedural means to only those who have a 'need-to-know'.** **Recommendation IR1-2: The police force should document an access policy for the data concerned which should include regular review of access privileges here.**
IR2. The system is hosted on an insecure infrastructure or premises. • Insufficient security could lead to unauthorised access internally or externally. This would lead to unauthorised data breaches which could lead to fines by the Information Commission Office (ICO). • There will be a personal impact experienced by the individuals who are subject to the data breach. • Reputational damage would occur within the Police Forces.	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	The system must be hosted on a secure IT infrastructure, either on police premises or hosted	**The Police systems from which data will be shared or received, will be accredited to national information security standards.** **Recommendation IR2-1: Police systems should be subject to information assurance/accreditation that should encompass technical and physical security aspects.**
IR3. People who should have access to the information have inappropriate levels of access to it	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Review technical, physical or procedural measures controlling access to the information on a regular basis and amend where necessary	**Recommendation IR2-1: Police forces to review technical, physical or procedural measures controlling access to the data on a regular basis and amend where necessary.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
IR4. The information is accidentally disclosed inappropriately	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Educate users on how to prevent the accidental inappropriate disclosure of the information Implement appropriate technical, physical or procedural measures to prevent accidental disclosure of the information	**Recommendation IR4-1: Police forces train users on how to prevent the accidental inappropriate disclosure of the data.** **Recommendation IR4-2: Police forces to implement appropriate technical, physical or procedural measures to prevent accidental disclosure of the data.**

IR5. The information is deliberately accessed or disclosed inappropriately	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Educate users on the criminal offences relating to deliberate access or disclosure of personal data (Section 170 Data Protection Act 2018) Educate users on the criminal offences within the Computer Misuse Act 1990 Implement auditing or validation of users' access and/or use of the information	**Recommendation IR5-1: Police forces to ensure users are trained in respect of their responsibilities relating to criminal offences relating to deliberate access or disclosure of personal data (Section 170 Data Protection Act 2018).** **Recommendation IR5-2: Police forces to train users on the criminal offences within the Computer Misuse Act 1990.** **Recommendation IR5-3: Police forces to implement auditing or validation of users' access and/or use of the data.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
IR6. The information is held or used in an insecure environment	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Conduct a risk assessment on the environment and implement appropriate technical, physical or procedural measures to protect the information	**Recommendation IR6-1: Police forces to conduct a risk assessment on the environment and implement appropriate technical, physical or procedural measures to protect the data.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
IR7. The information can be damaged or inappropriately deleted	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Review technical, physical or procedural measures concerning deletion or amendment of the information on a regular basis and amend them where necessary	**Recommendation IR7-1: Police forces to review technical, physical or procedural measures concerning deletion or amendment of the data on a regular basis and amend them where necessary.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
Integrity-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR8. The integrity of the information is jeopardised	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Review technical, physical or procedural measures concerning the integrity of the information on a regular basis and amend them where necessary	**Recommendation IR8-1: Police forces to review local arrangements will mitigate, through ensuring the integrity of IT systems on which the data will be processed.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
Availability-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR9. The information is inaccessible to those who should have access to it	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Review technical, physical or procedural measures controlling access to the information on a regular basis and amend them where necessary	**Recommendation IR9-1: Police forces to review technical, physical or procedural measures controlling access to the data on a regular basis and amend them where necessary.**
IR10. The information is not shared when it could be	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Review potential information sharing opportunities and adopt them where appropriate	**No action required.**
IR11. The information is not exploited when it could be	**1 Remote**	**1 Minimal**	**1 Low**	**Tolerate**	Identify and implement other appropriate potential uses of the information	**No action required.**

IR12. The information cannot be found (e.g. physical documents or searching of IT)	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Ensure the Register of Processing Operations and/or Information Asset Register is completed to record the location of the information Conduct periodic audits to test whether information can be found and undertake any necessary activities to improve the situation	**Recommendation IR12-1: Police forces to ensure the Register of Processing Operations and/or Information Asset Register is completed to record the location of the data.**
Legality-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR13. The purpose(s) for processing the information is unclear	**1 Remote**	**1 Minimal**	**1 Low**	**Tolerate**	Determine and record the precise reason(s) for processing the information, updating as is necessary	**No action required – lawful bases have been identified and are covered in this DPIA**
IR14. There is no lawful basis to process the information	**1 Remote**	**1 Minimal**	**1 Low**	**Tolerate**	Stop processing the information until a lawful basis for processing it is found Identify, record and regularly review the lawful basis for the processing	**No action required – lawful bases have been identified and are covered in this DPIA.**
IR15. The information is being used unfairly or without transparency to data subjects	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement physical or procedure measures to ensure transparency requirements are met – including consideration of a Privacy/Transparency Notice(s)	**Recommendation IR15-1: Police forces to use privacy notices, intranet news items and other internal comms to advise existing personnel of the HDW.**
IR16. The information is being used for a purpose incompatible with the reason it was first used/collected	**1 Remote**	**1 Minimal**	**1 Low**	**Tolerate**	Document the approved uses that the information may be put to Audit the use of the information to identify any incompatible use, which should be stopped	**No action required – the use of both datasets is not incompatible with the reason for collection and are covered in this DPIA.**
IR17. Pseudonymised versions of the information can be altered to identify individuals	**1 Remote**	**1 Minimal**	**1 Low**	**Tolerate**	Ensure any pseudonymisation information meets the requirements of appropriate published standards	**Not Applicable.**
Data Quality-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR18. The information is inaccurate	**1 Remote**	**3 Severe**	**1 Low**	**Treat**	Implement quality assurance processes when the information is first recorded Correct inaccurate data as soon as possible after it is apparent it is inaccurate	**Recommendation IR18-1: Police forces to Implement quality assurance processes when the data is first recorded or received with manual review prior to any further actions being taken.** **Recommendation IR18-2: Police forces to correct inaccurate data as soon as possible after it is apparent it is inaccurate.** **Similar measures will be imposed on the Processor through the Data Processing Contract (see IR28).**

IR19. The information is incomplete	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Implement quality assurance processes when the information is first recorded	**As above.**
IR20. The information cannot be amended when it needs to be	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Adopt processes to append new 'correct' information to the information requiring amendment Implement technical measures to allow the information to be amended	**As above.**
IR21. Duplicate versions of the information exist	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Adopt technical and procedural measures to prevent the creation of duplicate copies of the information Run audits to identify duplicate copies of the information Merge the duplicate copies of the information Educate users on the issues arising from duplicated information and the measures they must adopt to prevent the creation of duplicated information	**As above.**
Records Management-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR22. Excessive information is held	**1 Remote**	**1 Minimal**	**1 Low**	**Treat**	Review the scope of the information held and reduce the scope so that it is restricted to that necessary for the purpose it is held Train users on the scope of information that should be collected	**Recommendation IR22-1: Police forces to review the scope of the data held and where necessary reduce the scope so that it is restricted to the minimum necessary for the purpose it is held**
IR23. The information is held longer than is necessary	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Document the RRD processes	**Recommendation IR23-1: Police forces to document and implement review, retention and deletion (RRD) processes and policy (technical and/or non-technical) so that the data is retained no longer than is necessary.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**

					Educate users as to their responsibilities in connection with the RRD processes	
IR24. The information cannot be disposed of when no longer required	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement technical measures to allow the information to be disposed of	**Recommendation IR24-1: Police forces to implement technical measures to allow the information to be disposed of.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
Training-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR25. Users of the information are inadequately trained	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement appropriate training for all users	**Recommendation IR25-1: Police forces to implement appropriate training of all personnel involved in delivery of the HDW.** **Similar measures will be required by the Processor through the Data Processing Contract (see IR28 here).**
Governance-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR26. There is inadequate policy or procedure surrounding the access or use of the information	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement and maintain necessary policy or procedure concerning the access or use of the information	**Recommendation IR26-1: Police forces to implement and maintain necessary policy or procedure concerning the access or use of the HDW Data.**
IR27. There is an absence of an adequate information sharing agreement (where one is required)	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Implement and maintain necessary information sharing agreements and review these on at least an annual basis	**No data sharing agreement is required.**
IR28. There is an absence of a data processing contract (where one is required)	**1 Remote**	**3 Severe**	**1 Low**	**Treat**	Implement and maintain necessary data processing contracts	**Recommendation IR28-1. There will not be a contract for the provision of the HDW as this utilises the PND, however there is a described "Request for Change" which is exchanged between the Home Office who are responsible for the contracting of the PND and CGI who deliver that function..**
IR29. Generally there is inadequate governance for the information	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Designate, train and task an information asset owner for the information	**Recommendation IR29-1: Where necessary police forces to implement any missing governance measures including information asset ownership, policy, oversight and audit.**
Ethical-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR30. The information is inappropriately discriminatory	**1 Remote**	**2 Significant**	**1 Low**	**Tolerate**	Implement measures to ensure that the collection and use of the information does not inappropriately discriminate against certain groups, in particular children	**It is anticipated that the collection and use of the data will not inappropriately discriminate against certain groups and will comply and support the College of Policing Code of Ethics. The performance measures to be agreed by the NPCC will include some protected characteristics so that this can be assessed.**
IR31. Data Subjects are unaware of their rights regarding the information	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Ensure that Privacy/Fair Processing Notices provide details	**Recommendation IR31-1: Police forces to ensure that Data Subjects Rights to be set out in Privacy Notices.**

					of data subjects' rights and how to exercise them	**See IR15.** **.**
Miscellaneous	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR32. Logs are not maintained in accordance with DPA Part 3 Section 62;	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**		**Recommendation IR32-1: Police forces to ensure that any IT systems used by themselves or the Processor of the HDW satisfy the S62 requirements.**

.

Step 6: Assess Data Protection Compliance

The NPCC Data Protection Officer will complete this step with assistance from the Business SME, Business Lead and other associated Data Protection professionals, as is necessary.

The green text below has been added by the NPCC DPO based on the expectation that the recommendations arising from Steps 4 and 5 are adopted.

Processing for Law Enforcement Purposes

Law Enforcement 1st Principle (Lawful & Fair)

(DPA Part 3 Section 35)

Requirement	Compliant?
LE1. No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA)	**Yes.**
LE2. The processing is authorised by either statute, common law, royal prerogative or by or under any other rule of law	**Yes - Common Law Policing Purposes.**
LE3. Either of the following two processing conditions under DPA Part 3 Section 35(2) apply: Consent has been obtained, in compliance with ICO Guidance, or Processing is necessary for task carried out by a competent authority;	**Yes - Task carried out by a competent authority.**
LE4. Where **Sensitive Processing** occurs either of the two following cases exist: DPA Part 3 Section 35(4) - Consent has been obtained, in compliance with ICO Guidance and an appropriate policy document exists as per DPA Part 3 Section 42. or DPA Part 3 Section 35(5) - Processing is strictly necessary, an Appropriate Policy Document exists as per DPA Part 3 Section 42, and one of the following DPA Schedule 8 conditions is met: 1 Statutory etc. purposes 2 Administration of justice 3 Protecting individual's vital interests 4 Safeguarding of children and of individuals at risk 5 Personal data already in the public domain 6 Legal claims	**Yes - Processing is strictly necessary, police forces will have in place APDs and conditions 1 will apply i.e. the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and it is necessary for reasons of substantial public interest.**

7 Judicial acts 8 Preventing fraud 9 Archiving etc;	
LE5. The processing is in accordance with data subjects' reasonable expectations (fair); measures to provide privacy information are in place; Privacy Notices adequately describes the purpose and provide information about specific categories of processing including retention periods and transfers.	**Yes.**

Law Enforcement 2nd Principle (Specific, Explicit & Legitimate Purpose)
(DPA Part 3 Section 36)

Requirement	Compliant?
LE6. The purpose for collecting the personal data is specified, explicit and legitimate	**Yes – Various Law Enforcement Purposes as described within this DPIA.**
LE7. Processing is compatible with the purpose it was collected for	**Yes.**
LE8. Personal data collected for the law enforcement purpose is not otherwise processed unless it is authorised by law to do so	**Yes.**

Law Enforcement 3rd Principle (Adequate, Relevant & Not Excessive)
(DPA Part 3 Section 37)

Requirement	Compliant?
LE9. Adequate for the purpose	**Yes.**
LE10. Relevant to the purpose	**Yes.**
LE11. Not Excessive for purpose	**Yes.**

Law Enforcement 4th Principle (Accurate & Kept-up-to-date where necessary)
(DPA Part 3 Section 38)

Requirement	Compliant?

LE12. Is accurate with distinction between fact-based and opinion-based	**Yes.**
LE13. Is kept up-to-date where necessary	**Yes.**
LE14. Distinguishes between suspects, offenders, victims, witness & others where relevant	**Yes.**
LE15. Is erased or rectified if inaccurate without delay	**Yes.**
LE16. Is not transmitted or made available if inaccurate, incomplete or out-of-date	**Yes.**

Law Enforcement 5th Principle (Kept no longer than is necessary)

(DPA Part 3 Section 39)

Requirement	Compliant?
LE17. Personal data is not kept longer than is necessary	**Yes.**
LE18. It is possible to justify the retention in relation to the purpose of the processing	**Yes.**
LE19. A written retention, review and deletion policy exists for the personal data	**Yes (up to 12 months).**
LE20. Personal data is subject to periodic review and is anonymized, erased or disposed of when no longer needed	**Periodic review not required.**

Law Enforcement 6th Principle (Processed Securely)

(DPA Part 3 Section 40)

Requirement	Compliant?
LE21. Appropriate measures are in place or planned to prevent the personal data being accidentally or deliberately compromised	**Yes.**
LE22. Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach	**Yes.**
LE23. Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing	**Yes.**
LE24. Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification	**Yes.**

to the Commissioner and data subject) (DPA Part 3 Sections 67 and 68) involving the personal data	
LE25. DPA Part 3 Section 66 Security of processing requirements are met	**Yes.**

Law Enforcement Accountability Requirement
(DPA Part 3 Section 34)

Requirement	Compliant?
LE26. It is possible to demonstrate compliance with all the Law Enforcement Principles	**Yes.**

Other DPA Part 3 Controller & Processor Obligations
(DPA Part 3 Section 40)

Requirement	Compliant?
LE27. Compliance with Controller's general duties (DPA Part 3 Section 44)	**Yes.**
LE28. Appropriate technical & organisational measures, including policy as required by DPA Part 3 Section 56 are implemented;	**Yes.**
LE29. Data Protection by Design & Default requirements set out in DPA Part 3 Section 57 are met	**Yes.**
LE30. Where joint controllership exists that each parties' respective obligations under DPA Part 3 Section 58 to comply with the UK GDPR are documented	**Yes.**
LE31. Where a processor is employed DPA Part 3 Section 59 and 60 obligations are met including the requirement for a data processing contract to be place	**Yes.**
LE32. Records of processing activities are maintained in accordance with DPA Part 3 Section 61;	**Yes.**
LE33. Logs are maintained in accordance with DPA Part 3 Section 62;	**Yes.**
LE34. Data Protection Impact Assessments (DPIA's) are conducted in accordance DPA Part 3 Section 64 and 65 where required	**Yes.**

Law Enforcement International Transfers
(DPA Part 3 Section 37)

Requirement	Compliant?
LE35. Where the transfer is to competent authorities it is in compliance with DPA Part 3 Section 73 General principles for transfers of personal data, including where a third country is 'adequate' (DPA Part 3 Section 74) or where there are appropriate safeguards (DPA Part 3 Section 75), or special circumstances apply (DPA Part 3 Section 76). or Where the transfer is other than to competent authorities it is compliance with DPA Part 3 Section 77;	**Not Applicable.**
LE36. Conditions regarding subsequent transfers are set as required by DPA Part 3 Section 78.	**Not Applicable.**
LE37. Where the transfer is to competent authorities it is in compliance with DPA Part 3 Section 73 General principles for transfers of personal data, including where a third country is 'adequate' (DPA Part 3 Section 74) or where there are appropriate safeguards (DPA Part 3 Section 75), or special circumstances apply (DPA Part 3 Section 76). or Where the transfer is other than to competent authorities it is compliance with DPA Part 3 Section 77;	**Not Applicable.**

Processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes
(DPA Part 3 Section 41)

Requirement	Compliant?
LE38. Where this applies this is compliant with DPA Part 3 Section 41.	**Not Applicable.**

Processing for General Purposes

UK GDPR 1st Principle (Lawful, Fair & Transparent)
UK GDPR Article 5(a)

Requirement	Compliant?
G1. No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA/UK GDPR)	**Yes**
G2. One of the five available UK GDPR Article 6(1) **Processing Conditions** exists for all of the personal data	**Yes – (c) processing is necessary for compliance with a legal**

including Special Category Data and Criminal Offence Data *(Note: The Police are unable to use (f) Legitimate Interests)*: (a) Consent; (b) Contract; (c) Legal Obligation; (d) Vital Interests; (e) Public Task (see DPA Part 2 Section 8 for examples)	**obligation to which the controller is subject;** **(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.**
G3. If **Consent** is used it complies with definition at UK GDPR Article 4(11), requirements at UK GDPR Article 7 (Conditions for Consent), and ICO Guidance (subject to exemption for **Special Purposes** at DPA Schedule 2 Part 5 Paragraph 24);	**Not Applicable.**
G4. For any **Special Category Data** being processed, in addition to a UK GDPR Article 6(1) **Processing Condition** being met, one of the following UK GDPR Article 9(2) **Special Processing Conditions** applies: (a) Explicit Consent; (b) Employment, Social Security & Social Protection; (c) Vital Interests; (d) Political, Philosophical, Religious or Trade Union (e) Made Public by Data Subject; (f) Defence of Legal Claims; (g) Substantial Public Interest; (h) Health and Social Care; (i) Public Health; (j) Archiving, Research & Statistics **And** in the case of (b) Employment, Social Security and Protection, or (h) Health and Social Care, or (i) Public Health, or (j) Archiving, Research and Statistics, a condition in DPA Schedule 1 Part 1 applies; or in the case of (g) Substantial Public Interest, a condition in DPA Schedule 1 Part 2 applies And An **Appropriate Policy Document** is created and maintained in accordance with DPA Schedule 1 Part 4 if a condition in DPA Schedule 1 Part 1 or 2 is used	**Yes.**

G5. If the purpose of the processing differs from the initial purpose when the data was collected, and the processing is not based on consent or law, compatibility of the new use is tested using UK GDPR Article 6(4)	**Yes.**
G6. For any **Criminal Offence Data** being processed, in addition to a UK GDPR Article 6(1) **Processing Condition** being met; compliance with UK GDPR Article 10 is achieved; a DPA Schedule 1 Part 1, 2 or 3 is condition is met, an **Appropriate Policy Document** is created in accordance with DPA Schedule 1 Part 4; and the processing is authorised by law as a clear and foreseeable application of a common law task, function or power, a statutory provision, or statutory guidance	**Yes.**
G7. Fairness & Transparency requirements under UK GDPR Articles 12 13 14 are met	**Yes.**
G9. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified.	**Yes.**

UK GDPR 2nd Principle (Purpose Limitation)

UK GDPR Article 5(b)

Requirement	Compliant?
G10. Processing is in a manner that is compatible or where is for archiving in public interest, scientific or historical research or statistical purposes is exempt from that requirement by virtue of UK GDPR Article 89(1)	**Yes.**
G11. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2 **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3 **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26	**Yes – none required.**

UK GDPR 3rd Principle (Data Minimisation)

UK GDPR Article 5(c)

Requirement	Compliant?
G12. Personal data is adequate for the purpose(s) of processing	**Yes.**
G13. Personal data is relevant for the purpose(s) of processing	**Yes.**

G14. Personal data is limited to that required for the purpose(s) of processing	**Yes.**
G15. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2 **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3 **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26.	**Yes – none required.**

UK GDPR 4th Principle (Accuracy)

UK GDPR Article 5(d)

Requirement	Compliant?
G16. Personal data is accurate for the purpose(s) of the processing	**Yes.**
G17. Personal data is up-to-date where necessary for the purpose(s) of the processing	**Yes.**
G18. Personal data is erased or rectified without delay where required	**Yes.**
G19. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26.	**Yes - none required.**

UK GDPR 5th Principle (Storage Limitation)

UK GDPR Article 5(e)

Requirement	Compliant?
G20. Personal data enabling the identification of data subjects is retained no longer than is necessary for the purpose(s) of the processing,except where continued retention is solely for archiving in the public interest, scientific or historical research or statistical purposes in accordance with UK GDPR Article 89 & measures required by the UK GDPR are in place to safeguard the rights and freedoms of the data subjects.	**Yes (up to 12 months).**

UK GDPR 6th Principle (Integrity & Confidentiality)

UK GDPR Article 5(f)

Requirement	Compliant?

G21. Appropriate measures are in place to prevent the personal data being accidentally or deliberately compromised	**Yes.**
G22. Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach	**Yes.**
G23. Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing	**Yes.**
G24. Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) (UK GDPR Article 33 and 34) involving the personal data	**Yes.**
G25. UK GDPR Article 32 Security of processing requirements are met	**Yes.**

UK GDPR Accountability Requirement

UK GDPR Article 5

Requirement	Compliant?
G26. It is possible to demonstrate compliance with all the UK GDPR Principles	**Yes.**

Other UK GDPR Controller & Processor Obligations

Requirement	Compliant?
G27. Appropriate technical & organisational measures, including policy as required by UK GDPR Article 24 are implemented	**Yes.**
G28. Data Protection by Design & Default requirements set out in UK GDPR Article 25 are met	**Yes.**
G29. Where joint controllership exists that each parties' respective obligations under UK GDPR Article 26 to comply with the UK GDPR are documented	**Yes.**
G30. Where a processor is employed UK GDPR Articles 28 and 29 obligations are met including the requirement for a data processing contract to be place	**Yes.**
G31. Records of processing activities are maintained in accordance with UK GDPR Article 30	**Yes.**

G32. Data Protection Impact Assessments (DPIA's) are conducted in accordance with UK GDPR Articles 35 and 36j where required	**Yes.**

Where necessary, consider restricted transfers of personal data for general processing purposes to countries or territories beyond the European Union or to international organisations (**third countries)**

Requirement	Compliant?
G33. The restricted transfer is in compliance with UK GDPR Article 44 General principles for transfers of personal data, including where a third country is 'adequate' (UK GDPR Article 45) or where there are appropriate safeguards (UK GDPR Article 46, 47 or 48), or an GDPR Article 49 condition applies.	**Not Applicable.**

Step 7: Sign-off and record of outcomes

Consultation Outcomes

Summary of consultation responses (if conducted):

Not Undertaken

Summary completed by:

Not applicable

Date completed:

Not applicable

Business Lead's response to consultation responses (if conducted)

Not applicable

Date completed:

Not applicable

Data Protection Officer Comments

Data Protection Officer's comments, including whether the DPIA has been conducted appropriately and whether it must be sent to the ICO for review:

I am content that this DPIA has been conducted appropriately, with relevant Data Protection/privacy risks ascertained and suitable mitigations to those risks identified for consideration/adoption. I anticipate that many of those mitigations will have already been implemented by police forces as part of their pre-existing usual business processes.

In my view there is no requirement for this DPIA to be sent to the ICO for review as the risks surrounding the processing do not meet the threshold for referral to the ICO.

In the current absence of CC Kennedy I regard it as appropriate for the Chair of the NPCC to complete the Business Lead section below.

Should there be any significant deviation from the planned processing described in this DPIA or a Personal Data Breach occur I recommend this DPIA is reviewed and updated as is necessary.

Date completed:

2nd February 2023.

Business Lead's Comments

Business Lead's confirmation of agreement with risk assessment, acceptance of identified responses to risks, consideration of Data Protection Officer's comments and acceptance of responsibility to update this DPIA as is necessary.

In lieu of Chief Constable Serena Kennedy who is unavailable, I am reviewing this DPIA in my capacity as Chair of The National Police Chiefs' Council (NPCC). The completion of the DPIA has been overseen by our Data Protection Officer and I am satisfied that all elements are appropriately considered and answered. The HDW is critical work in terms of public trust and confidence in policing and has clear time parameters for completion. Importantly, the risk schedule at step 4&5 is comprehensive and the mitigating recommendations are clear.

Martin Hewitt QPM

Date completed:

3RD February 2023