Data Protection Impact Assessment (DPIA) – Stage 1

Template Version Control			
IMS Use Only			
Version	**Purpose/Change**	**Author and Role**	**Date**
1.0	Final version	Gary Brailsford-Hart – Director of Information Management Services (IMS)	DD/MM/YYYY
1.1	Revision of numbering in section 2.9. Formatting of detail/description area. Template and DPIA version controls added.	Jonathan Hands – Senior Information Officer in IMS	29/04/2020
1.2	Data flow diagram requirement added to 2.4 and structured requirements added to 2.5 and 2.11.	Jonathan Hands – Senior Information Officer in IMS	07/07/2020
1.3	Headings introduced to 2.1 for ease of understanding.	Jonathan Hands – Senior Information Officer in IMS	21/09/2020

DPIA Version Control			
Version	**Purpose/Change**	**Author and Role**	**Date**
			DD/MM/YYYY

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to refer to the guidance material available here 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:	
Information Asset Owner:	
Information Custodian:	
DPIA Coordinator:	
Date on which processing will commence:	DD/MM/YYYY
Date submitted to IMS:	DD/MM/YYYY
Note: IMS will give an **initial response** within 10 working days of receiving the completed form.	

IMS Assessment		
IMS Use Only		
A. DPIA is not mandatory.	☐	
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.

Aim and Purpose (policing, law enfocement, etc.);

Necessity;

Proportionality;

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.

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

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 COLP's possession, from a partner agency.

2.4.1 Information lifecycle / data flow diagram. Please provide a diagram or table indicating the flow of data within this proposal, from "cradle (source) to grave (deletion). This should reflect the information lifecycle.

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.
How the data will be used (intel development, prevent and/or detect crime, bring offenders to justice, etc.); **How the data will be recorded (online report, Niche, LAN drives, etc);** **How the data will be stored;** **Who it will be shared with;**
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 ☐ COLP 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 the COLP collect data that it has not previously collected or had access to? An example of new information is medical data, facial recognition, track and trace, etc.
☐ Yes ☐ No

2.9 Data Sharing **Does the processing involve:**	**Select one option**

2.9.1	Data being shared with third parties external to the COLP or recipients that have not previously had routine access to the information?	☐ Yes ☐ No
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 MoU, contract, or other sharing agreement in place with all parties with whom data will be shared?	☐ Yes – agreements in place ☐ Yes – agreements to be signed off following DPIA(s) sign off ☐ 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?

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.

Advantages of achieving the purpose;

Disadvantages to data subjects;

Balance;

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.

Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes):

Choose an item.

Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes):

Choose an item.

3.2 Further Special Category Lawful Basis If processing special category data (section 2.3) you must have identified a further lawful condition
Operational Data: The processing is strictly necessary (please tick to confirm) ☐ **AND** One of the following conditions applies (select from the list): Choose an item.
Administrative Data It is necessary for one of the following conditions (select from the list): Choose an item. **OR** It is in the substantial public interest (tick to confirm) ☐ **AND** for the following purpose: Choose an item.

Section 4 – Review, Retention and Disposal
4.1 Does the proposal have a review, retention and disposal process that complies with COLP 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 COLP IM document suite.
☐ Yes ☐ 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"*	☐ Yes ☐ No	Click here to enter text.

	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.		
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	Click here to enter text.
5.3	**Public monitoring?** *"Systematic monitoring of a publicly accessible area on a large scale"*	☐ Yes ☐ No	Click here to enter text.
5.4	**New technologies or techniques?** *"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"*	☐ Yes ☐ No	Click here to enter text.
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	Click here to enter text.

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	Click here to enter text.
5.7	**Data matching?** *"Combining, comparing or matching personal data obtained from multiple sources"*	☐ Yes ☐ No	Click here to enter text.
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 COLP investigation.	☐ Yes ☐ No	Click here to enter text.
5.9	**Tracking?** *"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"*	☐ Yes ☐ No	Click here to enter text.
5.10	**Targeting of children or other vulnerable individuals?** *"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.	☐ Yes ☐ No	Click here to enter text.

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	Click here to enter text.
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 an COLP recruitment process.*	☐ Yes ☐ No	Click here to enter text.
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	Click here to enter text.
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	Click here to enter text.

Please forward the completed form to IMS via the Data Protection mailbox account.

Data Protection Impact Assessment (DPIA) – Stage 2

Template Version Control			
IMS Use Only			
Version	**Purpose/Change**	**Author and Role**	**Date**
1.0	Final version	Gary Brailsford-Hart – Director of Information Management Services (IMS)	DD/MM/YYYY
1.1	Formatting of detail/description area. Additions to consultation groups. Template and DPIA version controls added.	Jonathan Hands – Senior Information Officer in IMS	29/04/2020
1.2	6.1 updated.	Jonathan Hands – Senior Information Officer in IMS	21/09/2020

DPIA Version Control			
Version	**Purpose/Change**	**Author and Role**	**Date**
			DD/MM/YYYY

In this stage of the DPIA process you must provide full details about the lifecycle of the data and the risks associated with the proposal. The information you provide will supplement the information provided in Stage 1.

The aim of this process is to identify and mitigate risks. If any **residual risks** to individuals are **high** then the ICO must be consulted before processing commences. This should be undertaken with the expertise of the COLP Information Management Services (IMS).

Section 6 - Impact
6.1 Expanding upon the purpose outlined in Section 2.1, please detail the intended effect of the processing on: the COLP; the data subjects; and society / the general public. Describe the benefits and disadvantages to each of the above.
Benefits to data subjects (suspects / victims); **Disadvantages to data subjects (suspects / victims);** **Benefits to society and general public;** **Disadvantages to society and general public;**

Section 7 - Information Lifecycle	
7.1 Diagrams and Tables Please insert a diagram or table that demonstrates the flow of data within this proposal. You should reflect the information lifecycle.	
7.2 Provide a full description of the information lifecycle	
Stage of Processing	**Description**
Collection Where does the data originate from, who will collect it, how will the data be obtained and how often?	
Storage Describe where and how the data is to be stored.	
Use Describe how the data will be used. Describe whether it involves new technology or novel processing.	

Access Describe who has access to the data throughout the life of the processing.	
Recording Describe the processes for recording the data.	
Processors Describe the use of processors. If a third party is being used then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?	
Sharing With which external organisation(s) is the data shared, what data is shared, and why? Describe any sharing that will occur within the COLP. Outline any national and international sharing or processing.	
Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate.	
Disposal Describe the process for disposal of data, including when and how.	
7.3 Assets Describe the assets that you intend to use.	
Hardware	
Software	
Networks	
Hardcopy / paper	
Any other relevant assets	

Section 8 - Consultation

You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data then you consider consulting them or their representatives.

8.1 Do you intend to consult data subjects?

☐ **Yes**

If yes then outline your plan in **Section 8.2** below together with details of consultation with other stakeholders.

☐ **No** If no then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 8.2** below.	Click here to enter text.

8.2 Consultation Action Log

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

- Data subjects
- The general public
- Union representatives
- Information Security
- IMS
- Other police forces
- Biometrics Commissioner
- College of Policing
- Human rights groups
- COLP Legal
- Operational Security Advisor (OpSy)
- Partner agencies
- Data processors
- Information Commissioner's Office (ICO)
- Home Office
- Surveillance Camera Commissioner
- National Police Chief's Council

Who	When	How	Outcome

Section 9 - Full Risk Assessment

Identify and Assess Risks

In this section you must detail **all** data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. **The assessment criteria outlined in italics in section 9.1 applies to all categories** in Section 9 and 10 i.e. for 'likelihood' you must always assess whether it is 'rare, unlikely, possible, likely or almost certain'.

Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point and you must ensure that all factors relevant to your proposal are considered. If you run out of space then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Examples of **risks to individuals** include**:**	Examples of **corporate risks** include:
• 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

You should identify **solutions** such as:

- Deciding not to collect certain types of data
- Reducing the scope of processing
- Reducing retention periods
- Taking additional technical security measures
- Following approved codes of conduct
- Restricting access to data
- Training staff to understand the risks
- Anonymising or pseudonymising the data
- Using different technology
- Using an alternative third party processor

9.1 Data Protection Principles

1. Fair and Lawful
- Do you need to create or amend a privacy notice?
- If processing on the basis of consent, how will this be collected and recorded?

2. Purpose Limitation
- Does the processing actually achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all COLP systems if required?
- Is the retention period necessary and proportionate?

6. Security
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights
- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to IMS.

9.1 Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm** *1 - Rare* *2 - Unlikely* *3 - Possible* *4 - Likely* *5 – Almost Certain*	**Severity of harm** *1 - Insignificant* *2 - Minor* *3 - Moderate* *4 - Major* *5 - Critical*	**Initial Risk** *High* *Medium* *Low*	**Mitigation / Solution** *Describe the mitigation and whether it will be implemented*	**Result** *Is the risk:* *- Eliminated* *- Reduced* *- Accepted*	**Residual Risk** *High* *Medium* *Low*

9.2 Data Sharing - including the involvement of other Controllers and Processors						
- What contracts, MOUs etc are in place or may be required? - What measures have you taken place to ensure third parties comply with Data Protection laws?			- What risks are involved with sharing data? - Is sharing necessary and proportionate? - Is the sharing of data being minimised?			
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**

9.3 International Transfers						
- Will data be shared with a third party based outside the EU? - If you will be making transfers, how will you ensure that appropriate safeguards are put in place?						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**

9.4 Additional Risk Factors Describe any further risks, ensuring that any risks not already identified are included.						
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**

Section 10 – Operational Data Risks - Additional Risks Relevant to Operational Data Only						
This section is only applicable to proposals involving operational data. **If you are solely processing administrative data then move to Section 11.**						
10.1 Data Logging 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 then will a log be retained of the following actions:						
• **Collection** • **Alteration** • **Consultation** • **Disclosure** • **Combination** • **Erasure**				☐ Yes ☐ No* ☐ Not applicable ***If you answered "no" then you must record this as a risk below.		
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**

10.2 Data Categorisation 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 suspects, 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* ☐ Not applicable If you answered “no” then you must record this as a risk below.

Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk**	**Mitigation / Solution**	**Result**	**Residual Risk**

Section 11 – Outcome and Review			
11.1 Outcome			
Item	**Name**	**Date**	**Notes**
Residual risks approved by:			
IMS/DPO advice provided by:			
Summary of IMS/DPO advice, including whether the ICO must be consulted:			
11.2 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.			
Outline: • Who will be responsible for reviewing the processing? • The frequency of review • The date of the next review			