CLEVELAND POLICE

OPCC Resolution Team
(handling of expressions of dissatisfaction)

[Project Number]
Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a mandatory requirement under the General Data Protection Regulations (GDPR). Publication improves transparency and can increase the public's understanding of how their information is used.

This document is disclosable under the terms of the Freedom of Information Act. No part of the report should be disseminated or copied without prior approval from the author. You must identify sections which you believe are not suitable for publication. Where it is perceived that there is harm in the disclosure, the documents should be forwarded to the FOI Unit for review. For further information as to what to disclose if required under FOI, please contact the FOI Unit.

VERSION CONTROL

Version	Date	Author	Reason for Change
1.0	15.09.2021	[redacted]	New complaints service

Introduction

A Data Protection Impact Assessment (DPIA) is a process which enables Cleveland Police to identify and address the likely privacy impact of a new initiative or project. It enables privacy considerations to be made in the early stages of a project where any identified problems can be easier to resolve rather than late or retrospective consideration where solutions can be more costly or delay implementation. It can also identify, following completion of the DPIA, whether the project should be continued when balanced with the rights of persons affected.

The responsibility for conducting the DPIA lies with the Information Asset Owner (IAO) for a project and is produced as part of the project proposal however; this activity can be delegated to an appropriate person such as the Project Manager/Lead. Once initiated please contact the Information Management and Compliance Department (Information Sharing Officer) who will arrange a brief meeting with relevant parties, this will normally include at least the Data Protection Officer, Information Sharing Officer and the Information Security Officer Force Data Protection Officer (DPO) to discuss the DPIA Process.

A project proposal can be an ideal base for a DPIA. The project proposal should explain how the project will benefit the organisation and links to the Police and Crime Delivery Plan.

The consideration of whether a DPIA is required is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal information.

The DPIA guidance and policy should be read in conjunction with the completion of this DPIA.

Upon completion of the DPIA template the Project Manager and IAO will review, sign off and send a copy to the Information Sharing Officer. The Information Sharing Officer will seek the views and approval of the Information Security Officer, the Risk and Business Continuity Management Advisor and the Data Protection Officer. The DPIA will then be considered and

signed off by the Senior Information Risk Officer (SIRO). The SIRO may at this point ask that additional work is carried out or may decline the proposal and not accept any risks identified. **If the DPIA identifies a high risk and measures cannot be undertaken to reduce the risk, then there is a requirement for the Force to consult with the Information Commissioner's Office (ICO). Consultation with the ICO will be undertaken by Information Management and Compliance staff under the supervision of the Data Protection Officer.**

This DPIA should be filled out at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into the project plan. The accompanying guidance document and the Force Data Protection Impact Assessment Policy should be referred to when undertaking the DPIA process.

The below process follows the process set out in the Information Commissioner's Office DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in the European guidelines on DPIA's (www.ico.org.uk).

Should you have any queries in relation to the Data Protection Impact Assessment Process then please contact the Force Data Protection Officer or the Information Sharing Officer within the Information Management and Compliance Department.

DOCUMENT CONTROL

System Owner	Business Lead	Information Asset Owner	Project Manager
Cleveland Police	[redacted]	Cleveland Police	[redacted]

Author	Role	Department
[redacted]	Project Manager	OPCC
Contributors	**Role**	**Department**

Version	Version date	Requester of change	Summary of change(s)
1.0	15.09.21	Cleveland Police	DPIA for new complaint service

DOCUMENT REFERENCES

Ref	Document Name	Version Number

Screening Questionnaire

The following questions are intended to help you decide whether a DPIA is necessary. The DPIA guidance document will assist you during the project lifecycle. Answering 'yes' to any of the following screening questions is an indication that a DPIA is required. You can expand on your answers as the project develops.

If there is no personal data involved then go to Section 8 – Conclusions.

"Personal data" means any information relating to an identified or identifiable living individual - Section 3(2) of the Data Protection Act 2018.

Does the intended processing of personal information involve any of the following?

	Intended processing	Yes	No
1.	Systematic and extensive profiling with significant effects?		x
2.	Large scale use of sensitive data?	x	
3.	Public monitoring?	x	
4.	New technologies (processing involving the use of new technologies, or the novel application of existing technologies (including AI)?		x
5.	Denial of service: 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?	x	
6.	Large-scale profiling: any profiling of individuals on a large scale?		x
7.	Biometrics: any processing of biometric data?		x
8.	Genetic data: any processing of genetic data?		x
9	Data matching: combining, comparing or matching personal data obtained from multiple sources.	x	
10.	Invisible processing: processing of personal data that has not been obtained direct form the data subject in circumstances where the data controller considers that compliance with Article 14 of		x

	the GDPR would prove impossible or involve disproportionate effort.		
11.	Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.		x
12.	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 there is an intention to offer online services directly to children.		x
13.	Risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals.	x	
14.	Any other processing which is large scale involves profiling or monitoring, decides on access to services or opportunities or involves sensitive data or vulnerable individuals.		x

Article 14 of the GDPR: Under Article 14 the Controller is required to provide the data subject with specific information when the personal data being processed has not been obtained from the data subject (see: https://gdpr-info.eu/art-14-gdpr/).

Even if there is no specific indication of likely high risk, a DPIA will be undertaken for any major new project involving the use of personal data.

The below criteria may act as indicators of likely high-risk processing:

- *Evaluation or scoring*
- *Automated decision-making with legal or similar significant effects*
- *Systematic monitoring*
- *Matching or combining datasets*
- *Processing of sensitive data or data of a highly personal nature*
- *Processing data on a large scale*
- *Processing of data concerning vulnerable data subjects*
- *Innovative technological or organisational solutions*
- *Processing involving preventing data subjects from exercising a right or using a service or contract*

In most cases a combination of two of the above factors will indicate the need for a DPIA; however, this may not always be the case. It may be possible to justify a decision not to carry out a DPIA if the IAO is confident that the processing is nevertheless unlikely to result in a high risk, however the reasons for not undertaking a DPIA will be documented. In some cases, it may be necessary to undertake a DPIA if only one of the above factors is present – it will be good practice to do so. A copy of the decision-making process for not undertaking a DPIA will be provided to the Information Management and Compliance Department.

Cleveland Police will consider carrying out a DPIA if the below criteria apply:

- *If there is a change to the nature, scope, context or purposes of our processing*

Step 1 – Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The Police and Crime Commissioner (PCC) has decided to take on fullest responsibility, made available to him under the Policing and Crime Act 2017 and Police (Complaints and Misconduct) Regulations 2020, for the handling of expressions of dissatisfaction against the police. Changes already effected last year included Office of Police and Crime Commissioner (OPCCs) becoming the Appropriate Authority for formal reviews of the handling and outcome of police complaints. The aim of the reforms was to provide a more transparent, more efficient complaints process with three distinct operating models that have increasing involvement from the local policing body (OPCC), the greatest of which is Model 3. Model 3 provides that the PCC becomes responsible for: • Receives and makes initial contact with complainant • Handles complaints outside of Schedule 3, and records complaints (Chief Constables are required to approve delegation of this responsibility to OPCCs) • Keeps complainants and interested parties updated and informed of outcome • Investigates complaints • Conducts formal reviews of complaints handled inside Schedule 3. • The new service will use the national Force Information System for handling of complaints and conduct matters, known as Centurion. Initial data entry, following receipt of a complaint, is undertaken by the OPCC onto Centurion, which acts as the central repository for management, logging associated enquiries and actions undertaken to resolve the complaint. The OPCC team will primarily use the Cleveland Police module upon the Centurion complaints system, albeit that certain Force restricted information will not be available to them, for the processing, i.e. logging and recording of complaints. Other systems that will be used include: NICHE – thius will be accessed on a read-only basis by the OPCC Resolution Advisors, to check

background details of the incident/ crime that complainants ae calling to express dissatisfaction about. Additionally, NICHE will be used for checking any safeguarding/ vulnerability issues of the complainant, that might warrant the Resolution Advisor providing a more immediate response.NICHE will lastly be used to check any warning markers that might indicate a a greater need for sensitive handling of the complainant.

Webstorm may occasionally be used where NICHE details do not provide sufficient clarifying detail of the incident/ crime.

Red Box – this is used to check voice recordings of calls made to call handlers within Force Control Room (FCR) where the complainant has specifically indicated they are unhappy with the service received from FCR. The system will be used to verify whether the complaint has merit.

Body Worn Video – Edesix Video Manager (within 30 days) and NICE Investigate (30 days +) – this is used to check Cleveland Police owned body worn footage of an incident/ crime that police have responded to, where the complainant has specifically indicated that they are unhappy with the service provided by the police during response. They system will be used to verify whether the complaint has merit.

E-Duty – for duty rosters

CP DMS Service and Duties –to ascertain hierarchy

Associated documents:

- A high-level business case is attached for reference.
- Process and data flow map
- An information sharing agreement and service level agreement is being developed.
- Process%20flow%20 1.5.docx

Step 2 – Describe the processing

Describe the nature of the processing:

How will you collect, use, store and delete data?

Members of the public are entitled in law to express a dissatisfaction against the police. They may do this via the following reporting routes:

- Telephone: 01642 xxxxxx (TBC - *currently in progress*). Calls can be answered during office hours by the ORT, and an answerphone facility will enable members of the public to leave a message if they

call out of hours. There will be a text-phone option for people with hearing loss.

- Email: Resolution@cleveland-pcc.gov.uk
- Letter: c/o St. Mark's House, St Mark's Court, Thornaby, Stockton-on-Tees, TS17 6QW.
- Online:
  - expressions of dissatisfaction against the Force may be made explicitly on the social media profiles (Twitter, Facebook, Instagram, or LinkedIn) for the OPCC and/ or Force.
  - expressions of dissatisfaction against the Force can be made via a webform on the OPCC website: https://www.cleveland.pcc.police.uk/contact/complaint/
  - use of the Single Online Home link on the Cleveland Police website which links to the OPCC webform: https://www.cleveland.police.uk/fo/feedback/tc/thanks-and-complaints/make-complaint/?lid=&cid=&rid=5&stepid=1-2-1
- In person:
  - By prior appointment (to mitigate risk to staff members) at Cleveland Police Headquarters, or elsewhere on the police estate if that better suits the complainant.
  - Unannounced visits from complainants to Cleveland Police HQ will also be facilitated where possible and where staff are available, but this service cannot be guaranteed thus will not be advertised. The team leader or another senior leader will risk assess all in person contacts with members of the public.
  - The ORT will not normally conduct home visits unless there are compelling circumstances, for instance a profound disability, which make it unfeasible for the complainant to travel to the nearest police estate to meet. This will be risk assessed and managed by the Team Leader or another OPCC senior leader.
  - to police officers or staff at front desk counters.
  - to police officers or Police Community Support Officers (PCSOs) on local patrols.
- Online/ in person:
  - by the complainant making use of a live connection platform such as Teams or Zoom

What is the source of the data?

Members of the public expressing a dissatisfaction with the service provided to them by Cleveland Police. They will volunteer the information at the start of the process.

Will you be sharing data with anyone?

In line with the regulatory framework, data provided by members of the public can only be shared between the OPCC, Cleveland Police, the IOPC and the complainant who has provided that information. An exception to this is where there may be safeguarding or serious crime concerns, and therefore permissive gateways such as S115 of the Crime and Disorder Act 1998, or Article 6 of UK General Data Protection Regulations, or Schedule 1 of the Data Protection Act 2018.

You might find it useful to refer to a flow diagram or another way of describing data flows.

Attached above.

What types of processing identified as likely high risk are involved?

There would be large scale use of sensitive data, by virtue of the fact that the OPCC staff will be using Centurion to log/ record details from members of the public who make individual complaints. That data could also be provided to the IOPC.

The outcomes data will be used for scrutiny work within the OPCC, and the demographic information (but not individually identifiying information) would be monitored and published from time to time, in line with OPCC transparency commitments to publish data on how it and the Force and performing. Special category data will be used to ensure a the Force and OPCC are providing a proportionate and accessible service, as well as complaints handling and outcomes, to members of the public in the police force areas we serve.

Data matching is likely to occur when a complainant divulges complaints information that would then be compared, by a complaints team advisor, against information held on Cleveland Police's NICHE (crime and incident recording) system.

Breaches of complainants' data during processing, by a complaints advisor, could feasibly cause personal risk to the complainant, jeapordising their health and safety.

For this reason, the OPCC staff will be required to be management vetted, and work within a secure environment that has restricted access, with sound baffling to reduce noise.

Access to Centurion is permitted only via licence and training so only those with permitted access may use that that system.

Describe the scope of the processing:

What is the nature of the data, and does it include special category or criminal offence data?

The data will be requested by the OPCC from members of the public who contact the OPCC to submit a complaint. The primary system routes used for members of the public to submit complaint data will be Single Online Home on the Force's website, via the webform on the OPCC website, or submitted directly via email to the Resolution@cleveland-pcc.gov.uk inbox on the OPCC Outlook 365 system. Complaints submitted via Single Online Home or the OPCC website will automatically forwarded into the Resolution email inbox.

The scope of data that will be requested, via the online routes, is set out in the IOPC's national recording form, a copy of which is attached. That form does include some special categfory data, e.g. ethnicity.

Should complainants make contact via telephone, letter or in person routes, their details will be passed to the Resolution Team who will then ask for the data fields as set out in the IOPC form.

In addition to personal data requested in the form, information may, on an individual basis, also be gathered from NICHE, Webstorm, Red Box, Body Worn Video – Edesix System (within 30 days of incident) and NICHE Investigate (30 days + post incident), E-Duty – for duty rosters, and CP DMS Service and Duties –to ascertain hierarchy. This will all be used as described above, in order to establish the facts of the complaint and police service being complained about.

It should be noted that the OPCC Resolution Team do not have control over the complaint details that will be disclosed to them. The information disclosed may include sensitive, safeguarding information and/ or information that indicates a criminal offence.

How much data will you be collecting and using?

This is a demand led service there the data being collected is an unknown quantity, but 2134 complaints were received by Cleveland Police last year, which equates to 533 contacts per month.

It is likely that the new service will result in an uplift in contacts, by virtue of the fact that communications will be published to notify internal and external stakeholders.

How often?

This is an ongoing service that will be provided.

How long will you keep it?

Data weeding will be conducted in line with national guidance (Lord Chancellor's Code of Practice on management of records under S46 of Freedom of Information Act 2000) and the OPCC's Record, Retention and Disposal Policy (copy attached). It supports compliance with legislation which requires records and information to be kept, controlled and accessible, such as the Data Protection Act 2018 (S2.4), the UK General Data Protection Regulations, Freedom of Information Act 2000, Audit Commission Act 1998, employment and health and safety legislation.

Data weeding will be completed manually by designated administration officers within the OPCC.

How many individuals are affected?

The service is demand led and the exact number of complainants that will make contact is therefore difficult to quantify, but all those who choose to make a complaint will be affected.

What geographical area does it cover?

Cleveland Police force area.

Describe the context of the processing:

What is the nature of your relationship with the individuals?

Complainants will be service users who are likely to have had prior direct or indirect contact with Cleveland Police, who have witnessed service delivery they feel needs to be reported.

How much control will they have?

The complainant chooses to make the complaint. While they may request that their details are not recorded, this could be unavoidable if they disclose serious safeguarding or criminal matters within the course of the discussion with the OPCC staff member that the staff member is then obliged to disclose. This will be included in the privacy notice. They will also be advised, within the notice and by OPCC staff, of their rights in respect of Subject Access Requests.

If making a complaint to police front desk staff, staff will show the complainant a sign that advises them that the OPCC will be the data controller for the purposes of handling their complaint, and that they can gain more information on their rights via the OPCC website.

Would they expect you to use their data in this way?

Members of the public are likely to expect that this is reasonable and proportionate within the bounds of handling a complaint against the police. This will be explained to them and included in the privacy notice.

Do they include children or other vulnerable groups?

There is potential that service users may include children or other vulnerable groups, though it is predominantly adults who contact the complaints service presently.

Are there prior concerns over this type of processing or security flaws?

None recognised at this time.

Is it novel in any way?

No – the legislation was introduced last year and affects all police forces and OPCCs.

What is the current state of technology in this area?

Centurion is the national complaints against police recording system and the primary repository for data collection and managing complaints and discipline.

Are there any current issues of public concern that you should factor in?

None identified at this time.

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Yes, the OPCC-led service will operate in line with the Code of Ethics and College of Policing Approved Professional Practice frameworks.

Describe the purposes of the processing:

What do you want to achieve?

The intention is to create an effective customer focussed service in partnership with Cleveland Police Department for Standards and Ethics (DSE). The process will involve the logging of expressions of dissatisfaction, occasional recording, in line with national and local requirements and to enable a seamless service to be provided by the OPCC and DSE which will benefit the public, and strengthen police legitimacy with the public.

What is the intended effect on individuals?

To provide a transparent, robust and effective complaints system so that members of the public have the trust and confidence to report matters which will ensure as an organisation, that we are able to identify learning opportunities and act on these accordingly.

What are the benefits of the processing for you, and more broadly?

It will ensure the right data is captured in the right way, enabling proper and customer focussed service delivery.

Step 3: Consultation process

Consider how to consult with relevant stakeholders:

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Extensive consultation was undertaken prior to the introduction of the legislation and new regulations as

part of the Chapman review. Targeted local consultation has been undertaken on the proposed complaints model for Cleveland, which is set out in the business case.

A communication strategy has also been developed to ensure that all officers and staff are apprised of the changes, (in line with IOPC requirements), and to advise members of the public.

Who else do you need to involve within your organisation?

Internal key stakeholders are represented at the weekly working group:

- OPCC (including Data Protection Officer)
- DSE
- Information Security Officer
- Cleveland Police Head of Information Management and Data Protection Officer

Do you need to ask your processors to assist?

Yes – Centurion are a processor and will need to be requested to assist in respect of access permissions to the system, management/ retention of information.

Do you plan to consult information security experts, or any other experts?

Yes – the Data Protection Officer for the OPCC, the Head of Information Management and Data Protection Officer for the force and Information Security Officer for the Force will be consulted for their view and input.

Step 4 – Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

What is your lawful basis for processing?

Cleveland Police Chief Constable and Cleveland PCC will process this data, through delegated authorities, using the following legal bases:

GDPR Article 6 (1) (c) processing is necessary for compliance with a legal obligation: namely the Police Reform Act 2002
GDPR Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the official authority vested in the controller.
Special category data is processed using the following legal bases:
GDPR Article 9 (2) is necessary for substantial public interest
Data Protection Act 2018 Schedule 1 conditions:

6. Statutory and Government purposes
8. Equality of opportunity or treatment
10. Preventing or detecting unlawful acts
11. Protecting the public against dishonesty
12. Regulatory requirements relating to unlawful acts and dishonesty.

Where the processing of complaints leads to investigations and potential criminal activity, the Chief Constable will process this data as per the definition of law enforcement data at S31 of the Data Protection Act and in accordance with S35 of the Data Protection Act.

Does the processing actually achieve your purpose?

Yes. It is necessary for the handling of complaints against police.

Is there another way to achieve the same outcome?

There isn't one that can be identified.

How will you prevent function creep[1]?

The service level agreement which includes standard operating procedures, and other associated documents is explicit on the service that will be provided. It will act as the mainstay in ensuring demarcation between the role of the OPCC and the role of the Force in handling of complaints. In addition, data use and information governance will form part of the regular strategic monthly meetings that will be held between the OPCC and the Force. How will you ensure data quality and data minimisation?[2]

The project has built in regular review periods to di sample and cross reference to the service level agreements.

What information will you give individuals?

Information harvesting will be in line with other functions across the organisation. The complaints system will be a bespoke system and complaints advisors will provide advice and guidance to enable the complaints system to be navigated. Updates will also be provided by agreement with the customer and in accordance with the IOPC statutory guidance.

Posters, leaflets and external comms will also be produced.

[1] Function Creep – "*The gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy*".

[2] Data Minimisation – GDPR – Article 5 (1) (c) - Data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"*

Privacy notices will be published on the Cleveland Police and OPCC websites. Privacy information will also be provided at point at contact – via the online or in person mechanisms. Furthermore, privacy information will be provided during contact and correspondence with the complainant.

How will you help to support their rights?

OPCC and Cleveland Police systems have been developed to uphold the following rights:

- Right to be informed
- Right to access
- Right to request rectification and erasure
- Right to restrict processing
- Right to data portability
- Right to object to automated decision making
- Right to complain

The OPCC staff will also be trained in general data protection regulations, data protection and information management legislation, human rights, freedom of information, and subject access requests.

What measures do you take to ensure processors comply?

The system can be audited, and this will be done from time to time by the OPCC Resolution Team Leader, Data Protection Officer, and Monitoring Officer. OPCC and DSE staff also have anti-corruption software installed on their equipment, which monitors keystrokes etc. which DSE may utilise to dip sample OPCC usage of systems to ensure information accessed has been necessary for complaint handling as per the Data Processing Contract.

A data processing contract is being developed to enable OPCC staff to access Cleveland Police systems to obtain the information to be lawfully shared.

Centurion is a data processor – they will be covered by a data processing contract.

How do you safeguard any international transfers?

Centurion do not transfer information internationally.

Centurion operates a workflow system which manages transfer of data from user to user, and from OPCC to DSE. All information is restricted within one area.
In addition, the anti-corruption software that is installed on all Cleveland Police issued ICT (including the ICT used by the OPCC) should mitigate against any attempts to transfer or ensure early detection if such a breach is deliberately orchestrated.

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. Risk of OPCC staff having access to more information on Centurion than is necessary to perform the role on a complaint by complaint basis.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
2. Risk of OPCC having access to systems to gather information to allow them to triage and handle the complaint. Need to ensure process is set up for OPCC to request relevant information from Cleveland Police, and Cleveland Police will provide this. This will also be documented in the Information Sharing Agreement and DPC.	Possible Probable	Minimal Minimal	Low Medium

See the Force Risk Management section on the Intranet for further information regarding risk management.

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
1. Risk of OPCC staff having access to more information on Centurion than is necessary to perform the role on a complaint by complaint basis.	This risk is reduced by Cleveland Police's management of the Centurion modules, which restricts the visibility and accessibility of information that the OPCC staff can view. They are only able to partly view content related to cases they are currently working on.	Eliminated, reduced or accepted Reduced	Low, medium or high Low	Yes/no

2. Risk of OPCC having access to systems to gather information to allow them to triage and handle the complaint. Need to ensure process is set up for OPCC to request relevant information from Cleveland Police, and Cleveland Police will provide this. This will also be documented in the Information Sharing Agreement and DPC.	Risk reduced by putting a data processing contract in place, which will document what the OPCC are authorised to access within NICHE, Webstorm, Red Box, Body Worn Video – Edesix Video Manager (within 30 days of incident) and NICE Investigate (30 days + post incident), E-Duty – for duty rosters and CP DMS Service and Duties –to ascertain hierarchy . Other sharing on a controller to controller basis will be documented in an information sharing agreement.	Reduced	Low	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion

Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	[redacted] **24th Sept 21 DPO for Chief Constable**	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: **DPO for Chief Constable remarks – happy with the content and the arrangements documented within the DPIA. The DPO will pursue a data processing contract to cover the elements of system access performed on behalf of the dtaa controller. The OPCC will pursue an information sharing agreement to cover the lawful sharing of data.**		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Step 8 - Conclusions

Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with the DPA. Includes references to any changes that were introduced as a result of the DPIA process.

Sign-Off Authority	Role	Date	Signature
	Information Asset Owner		
	Project Manager		
	Information Security Officer		
	Data Protection Officer		
	Risk and Business Continuity Management Advisor (as required)		
	Senior Information Risk Owner (SIRO)		

Freedom of Information Act 2000

The Information Commissioners Office (ICO) encourages the publication of material relating to Data Protection Impact Assessments (DPIA). Publication improves transparency and can increase the public's understanding of how their information is used.

There is a requirement therefore to review this document to establish its suitability for publication. Please identify below whether the document is suitable for publication in its entirety or not. Where it is believed that disclosure will be harmful please articulate the harm that publication would cause and highlight the relevant sections within the document. Where it is perceived that there is harm in disclosure the document should be forwarded to the FOI Unit for review.

Suitability for publication

Suitability for publication	Yes/No	Date	Signature
Document is suitable for publication in its entirety			

Document is suitable for publication in part, I have identified those sections which I believe are not suitable for disclosure and have articulated below the harm which would be caused by publication.			
Harm – in publication			

FOI review – to be completed by FOI Unit

Suitability for publication	Yes/No	Date	FOI Decision Maker
Document is suitable for publication in its entirety			
Document is suitable for disclosure in part and relevant redactions have been applied. A public facing version has been created.			
Once review has been undertaken FOI decision maker to return document to DPIA author and following sign–off document to be published on the Cleveland Police website. Any future changes to the document should be brought to the attention of the FOI Unit, as appropriate.			