Law enforcement processing: Part 3 Appropriate Policy Document template

Part 3 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement (LE) purposes.

Sensitive processing is defined in Part 3 section 35(8) and is equivalent to GDPR special category data. This includes:

a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
c) the processing of data concerning health;
d) the processing of data concerning an individual's sex life or sexual orientation.

Processing for LE purposes must comply with the data protection principles outlined in Part 3 of the DPA 2018. Specifically, the first data protection principle (section 35) states that processing for LE purposes must be lawful and fair. In addition, you may only process sensitive personal data for LE purposes if you have an APD, and if the processing:

- is based on the consent of the data subject - section 35(4);

  or

- is strictly necessary for the LE purpose and is based on a Schedule 8 condition - section 35(5).

This document should demonstrate that the processing of this sensitive data is compliant with the requirements of Part 3 section 42 of the DPA 2018. Section 42(2) specifies that for the above processing, the APD should:

(a) explain your procedures for securing compliance with the LE data protection principles;

(b) explain your policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

If you conduct sensitive processing for several different LE purposes you do not need a separate policy document for each condition or processing activity – one

document can cover them all. You may reference policies and procedures which are relevant to all the identified processing.

This Part 3 APD complements your general record of processing under section 61 in Part 3 of the DPA 2018 and provides any sensitive processing with further protection and accountability. See Part 3 section 42. Note section 42(4) outlines the obligations of data processors.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge.

Note your APD does not have to be structured in accordance with this document. This template is intended as a guideline only.

Description of data processed

Give a brief description of each category of sensitive data processed. You may wish to refer to your section 61 record of processing for that particular data:

PND will process sensitive data, where it is necessary for law enforcement investigations. PND will process sensitive personal data on:

- race and ethnic origin
- religious or philosophical beliefs
- biometrics – facial images
- health data
- data related to sexual preferences, sex life, and/or sexual orientation.
- criminal convictions and other out of court disposals
- arrests and charges

PND has a facial search function which is used for post event image searching for intelligence purposes, (when a law enforcement purpose is identified).

The software used for facial searching uses an algorithm which compares images of people, (probe image) against lawfully held images (reference images). Reference images are of individuals who have been detained in a police custody centre, under the Police and Criminal Evidence Act 1984. It compares the probe image to the refence set of images and identifies possible matches using facial characteristics.

All matches are treated as intelligence, they are not evidential, and trained PND users Investigators must assess results before taking any positive action.

How facial images are processed

Each reference image uploaded to PND or used as a probe image for a facial search, is assigned an algorithmic template that is determined based upon the various dimensions of the face (e.g., between eyes, nose, chin, ears etc) which is then turned into a reference number.

Only forward-facing facial images should be used (where both ears can be seen) as the PND searches for possible matching images based upon the measurements between certain points on a face.

An algorithm is used for the matching, where it searches the probe image against the refence image set to find images which may match or have a similar template.

The match-score response on facial searches is based upon how closely the templates of the probe image and the reference set image match and not necessarily how likely the two images are to be of the same person.

Facial Search in the PND cannot say for definite if any two images are of the same person, but it suggests potential matches to PND users.

The facial search results returned are for those images that have the same reference number assigned to them (i.e., that also contain the same measurements between the various points on the face).

This can explain why in some cases female images can be returned for searches on a male image and vice versa, or persons of a different age and or ethnicity.

Probe and reference Facial images are enrolled into the database using software. The reference set will continually change as images are uploaded and deleted from source systems.

The software filters ensure only facial images of sufficient quality are enrolled.

Operational context for the processing

Operational requests for facial search can originate from several sources, the provenance of each image presented is established to ensure a policing purpose exists before the search is completed. Examples of probe images could be images of suspects obtained from CCTV, doorbell cameras, body worn cameras or provided by the public. Images are normally gained as part of a criminal investigation but can also be gained to help safeguard people.

The 'probe' image of the person to be identified or searched is uploaded into the PND by a trained PND user. The software compares the image of the unknown person, to the reference database. Where a possible match or matches are identified these will be returned to the trained PND user for further assessment.

Additional human safeguards are applied by the PND user who will visually assess the matches along with an investigator. The images which are visually identified as not a match to the probe image are discounted. The remaining match(es) are treated as intelligence and their value assessed by the investigator based on their knowledge of the investigation and other lines of enquiry.

No automated processing is completed once the facial search results are presented to the PND user. From this point forward, a person will decide how to use and manage the image within the context of the investigation. They will also consider the appropriate Codes of Practice, *CPIA 1996, ECHR and other relevant legislation.

*Criminal Procedure & Investigations Act 1996 Code of Practice (section 3.5):

In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the circumstances.

Reference dataset
The reference dataset contains lawfully held police images. The source of these images are people who have been arrested and or detained at a Police Custody centre. Images are collected under Section 64A of the Police and Criminal Evidence Act 1984 ('PACE') - the power to take facial photographs (known as 'custody images') of anyone who is detained following arrest.

The regime governing the review, retention and deletion of police images is set out by the College Policing within Authorised Professional Practice, (APP) for police information.

Consent or Schedule 8 condition for processing

For the specific sensitive data you are processing for LE purposes, explain whether you are relying on consent or a specific Schedule 8 condition for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

Processing data within PND for law enforcement purposes is strictly necessary and satisfies one of the eight conditions for sensitive processing in schedule 8.

The processing will not rely on consent.

Facial images used for searching are obtained under Section 64A of the Police and Criminal Evidence Act 1984 and/or they are obtained during an investigation.

The data protection lawful basis for the original collection of images which form the reference database are obtained in accordance with Section 35(2)(b) of the Data Protection Act 2018 *(The processing is necessary for a task carried out for a law enforcement purpose by a competent authority)* - this task being underpinned by S64A, PACE.

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of Part 3 of the DPA 2018 and in particular the principles. The sensitivity of the data means the technical and organisational measures you have in place to protect it are crucially important.

The questions are intended to help you describe how you satisfy each principle generally. They are not exhaustive and are only intended to act as a guideline. **The questions are broadly based on the requirements of each principle.**

In explaining your compliance with the principles, you should consider the specifics of your processing with respect to the specific data you have identified above.

There is also no requirement to reproduce information which is recorded elsewhere – **questions may be answered with a link or reference to other documentation, to your policies and procedures, your Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle

(i.) Do we maintain appropriate documentation of our processing activities?

Yes –, PND includes auditing capabilities. All activities within the system and access to it, have a mandatory logging functionality. This is in accordance with s.62 DPA. Logs for PND will be kept for at least the:

- collection
- alteration

- consultation
- disclosure (including transfers)
- combination; or
- erasure

This will include the details of searches and other data retrieval, for what was done and when it occurred. The logs are available to local auditor's, national auditors and the ICO, if requested.

Facial searches are audited and monitored as part of the overall audit responsibilities.

The activities of auditors, themselves, will be logged and subject to audit by the national auditors.

(ii.) Do we have appropriate data protection policies?

Yes – PND has a DPIA, Codes of Practice and a Manual of Guidance which all consider and follow the relevant DP policies. They clearly describe the Data protection responsibilities, expectations and explain how data will be processed and managed. The Codes of Practice clearly outlines the policing purposes which must be met to justify and compete a PND search. The Manual of Guidance provides guidance on all the searching functions within PND, including facial searching.

(iii.) Do we keep logs in accordance with our obligations under section 62?

Yes – PND has an audit function which is described in (i.) above.

In addition to audit, there are a number of measures in place which help to demonstrate compliance of the DPA, GDPR and their principles. We have a governance structure through the PND National Steering Group, PND Program Board which is led by the NPCC PND lead and Home Office Senior Responsible Officer. They are supported by Information Assurance specialists, the NPCC National SIRO and other appropriate NPCC leads.

PND users undertake mandatory vetting, training, audit and monitoring. All PND users are informed on their training and reminded they have responsibility for ensuring that data is processed in accordance with the DPA.

Principle (1): lawfulness and fairness

i. If the processing is relying on a Schedule 8 condition, is the processing strictly necessary for the identified LE purposes?

Yes – Processing of data within PND is strictly necessary for Law Enforcement purposes as defined in Part 3 of the DPA, 'for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.

ii. If we are relying on consent for processing, are we satisfied that the consent is valid?

Consent will not be relied upon.

iii. Do we make appropriate privacy information available with respect to the sensitive data?

Yes - A Privacy Impact Assessment was completed and published in 2018. The PND Manual of Guidance, PND Codes of Practice and DPIA are also available.

Principle (2): purpose limitation

i. Have we clearly identified our LE purpose(s) for processing as outlined in section 31?

Yes – Our LE purpose(s) for processing is aligned to section 31 DPA. The processing is required for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

ii. Are our purposes for LE processing specified, explicit and legitimate?

Yes – Competent authorities with the DPA have a common law or statutory duty to protect the public and share data to improve how we safeguard people from harm, investigate crime and prevent threats to public security.

iii. If we process sensitive data for a new LE purpose, do we ensure the new processing is authorised by law and is necessary and proportionate?

Yes – Any new processing will be considered by the NPCC PND lead, supported by Information Assurance specialists. New processing will be

documented and agreed considering the PND Joint Controllers Agreement, Data Sharing Agreements and DPIA's. These which will be developed, agreed and reviewed through appropriate governance.

iv. If we plan to use sensitive data for a new purpose other than LE purposes, do we check that the processing is authorised by law and also meets the requirements of the GDPR and DPA 2018?

Yes – PND will process data for other policing purposes, such as safeguarding responsibilities, captured for the purpose of general data processing under Part 2 DPA. The PND DPIA includes the assessment regarding part 2 processing. Any new purposes would be assessed within a DPIA which would be reviewed through NPCC PND governance.

Principle (3): data minimisation

i. **Are we satisfied that we only collect sensitive data we actually need for our specified purposes and that it is proportionate**?

Yes – The data collected and processed within PND only contains the relevant fields competent authorities need to fulfil their statutory requirements and the purposes within Part 2 and Part 3 of DPA.

Facial images are only collected and processed for lawful purposes.

ii. Are we satisfied that we have sufficient sensitive data to properly fulfil those purposes?

Yes – Data is supplied by joint controllers and controllers, uploaded direct from source systems. The loading service operated by the Home Office ensures data quality and validity before data is ingested into PND.

Facial images must meet a strict criterion before they are enrolled into the database and used for facial searching.

iii. **Do we periodically review this particular sensitive data, and delete anything we don't need**?

Controllers of source systems must have review and retention policies for their data following the Authorised Policing Practice for Police Information.

The PND DPIA details how review, retention and deletion occur within the PND. In summary the PND is a mirror of the data held in source systems, PND does not have an RRD function.

The PND portfolio are engaged with National Policing Leads to determine the most effective way to manage police images locally and nationally.

When a recommendation is agreed by policing leads, the PND DPIA and APD will be reviewed and updated.

Principle (4): accuracy

i. Do we have a process in place to identify when we need to keep the sensitive data updated to properly fulfil our purpose, and do we erase or rectify inaccurate data as necessary without delay?

PND mirrors the data held in source systems which upload data. The controllers of the source systems are responsible for reviewing and deleting records. When records are deleted or reviewed in the source system within a very short amount of time the PND database is automatically amended.

The PND DPIA provides more detail on the review and deletion process.

A PND Landscape Assurance team supports Police Forces to identify and rectify data quality issues.

ii. Do we distinguish between sensitive personal data based on facts and sensitive personal data based on personal assessments (opinion)?

Yes – The data contained within PND will be based on fact but will also include intelligence reports. Intelligence reports will contain an evaluation on the source and the intelligence. The evaluation will be recorded as per the 3x5x2 process as approved by the College of Policing Intelligence Management Authorised Professional practice (APP).

Intelligence evaluations are based on an assessment completed by the originating officer or member of staff.

iii. Where relevant and as far as possible, do we distinguish between sensitive personal data relating to different categories of data subject, as outlined in section 38(3)?

Yes – PND contains categories that distinguish the different categories of data subjects, as outlined in section 38 (3)

- 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.

The PND DPIA outlines the categories of data subjects that exist in PND

iv. Do we meet the verification requirements under section 38(5) for the transmission of data?

Yes – The load service completes verification before data is ingested into PND.

The load service is managed by a provider, who have been accredited by Police Digital Services and are employed by the Home Office who are responsible for the operational delivery and development of PND.

Details are included within the PND DPIA and the PND Business and Technical Guidance, (BTG).

Principle (5): storage limitation

i. Do we carefully consider how long we keep the sensitive data for the purpose for which it is processed and can we justify this amount of time?

Data within PND is populated from the source systems of the PND joint controllers and controllers. These systems have review and retention policies and sensitive data will be deleted when the source system identifies it is no longer required.

ii. **Have we established appropriate time limits for the periodic review of the need for the continued storage of this sensitive personal data**?

Retention of data is governed by the process followed by the controllers of the source systems. The regime governing the retention of custody images is set out in the Authorised Professional Practice for Police Information.

Principle (6): security

i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?

The PND can only be accessed by vetted and trained users. Users are restricted in number, (using a licensed model) and have access levels depending on their roles and vetting.
Assess control levels are used to protect access to the most sensitive data and user access is regularly reviewed.
Data is held on secure servers that comply with necessary security arrangements.
Police Digital Services provide the assurance for the PND, assessing and reporting risks and mitigations to the NPCC PND lead and National NPCC SIRO when required.

The Home Office provided specialist resources to continually assess, develop and respond to security issues.

ii. Do we have an information security policy (or equivalent) regarding this sensitive data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?

PND has a Manual of Guidance which is reviewed annually. All Police Forces and agencies who have access to PND must follow the Manual of Guidance, the DPA, ECHR and other relevant legislation.

iii. Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing?

Access to PND is protected through a secure gateway (IAM) which requires vetting and trained users to log in securely. Access to sensitive information is restricted based on the role and/or agency of the user. Access can only be gained using approved and secure IT devices and systems hosted by competent authorities and controllers.

PND has an audit regime to prevent and identify misuse.

Processing of facial images is managed using the accredited and tested data load service and the facial search engine.

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of sensitive data (this could include a link to your retention policy if you have one). You need to explicitly confirm how long you will retain each specific category of sensitive data, especially if the data no longer has any operational value.

Retention and erasure policy for the categories of data is aligned to the Authorised Professional practice for Police Information from the College of Policing.

Controllers who provide their data into PND have a responsibility to review, retain and delete records when appropriate. When the data in a source system is deleted, PND will receive an update to delete the corresponding record.

Information management | College of Policing

As of 2023 the PND portfolio engaged with Policing leads to improve how Policing manages images. The timescale for when policing will decide on a new regime for RRD for custody images is not known but when a decision is made the PND DPIA and APD will be reviewed and updated.

APD review date

25th August 2023

1st September 2024

15th November 2024

1st September 2025

26th November 2025