

Appropriate Policy Document

Part 3 Law enforcement processing

Guidance for Completion

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 UK GDPR special category data. This includes:

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

Purposes for processing

The following is a broad description of the purposes for processing of personal information:

- *victims of crime*
- *witnesses to crime*
- *people convicted of an offence*
- *people suspected of committing an offence*
- *complainants, correspondents and enquirers*
- *advisors, consultants and other professional experts*
- *suppliers*
- *current and former employees, cadets, agents, temporary and casual workers, and volunteers*
- *CCTV and BWV recordings*
- *representatives of individuals in this list, such as parents, other relatives, guardians, and people with power of attorney*
- *Intelligence gathering*
- *Research and statistical requests for Home Office and other bodies*
- *Custody and Biometric data (including Fingerprints, DNA, Photographs)*
- *Contracts and Vetting of Staff and Officers*
- *Training and development records*
- *Audit*

Categories of Individuals

- *Offender, Suspect, Victim, Witness details (including children)*
- *Individuals under surveillance (Overt and Covert)*
- *Crime details, including witness statements*
- *Employees, including staff, agency, contractors and volunteers*
- *Suppliers*
- *Complainants, enquirers and correspondents*

What types of personal data do we process

- *personal details (such as name, address and biographical details)*
- *family, lifestyle and social circumstances*
- *education and training details*
- *racial or ethnic origin*
- *political opinions*
- *religious or other beliefs of a similar nature*
- *trade union membership*
- *physical or mental health or condition, both declared and suspected*
- *sexual life*
- *offences (including alleged offences)*
- *criminal proceedings, outcomes and sentences*
- *physical identifiers (including DNA, fingerprints and other genetic or biometric samples)*
- *sound and visual images (e.g. from body worn cameras, CCTV, or facial recognition software)*
- *financial details*
- *goods or services provided*
- *licences or permits held (e.g. driving licences or firearms certificates)*
- *criminal intelligence*
- *information identifying user vulnerability, persistent targeting, and/or hate crime status*
- *references to manual records or files*
- *information relating to health and safety*
- *complaint, incident, and accident details*
- *opinions and assessments of officers and staff in relation to individuals dealt with*

The types of personal data we process will vary depending on the purpose. We aim to process the minimum amount of personal data necessary for the relevant purpose

Consent or Schedule 8 condition for processing

Sussex Police and Surrey Police will process vast amounts of data for the purposes of:

- *Protecting life and property;*
- *Preserving order;*
- *Preventing the commission of offences;*
- *Detection of future crime;*
- *Bringing offender to justice, and*
- *Any duty or responsibility arising from common or statute law.*

The Police will process Personal / Special Category Data under Police's statutory functions and where processing is necessary for the performance of a task carried out for that purpose by a competent authority. The definition of statutory function for 'law enforcement purposes' is '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.

In addition, the police will share Special Category data where the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions in Schedule 8. For this reason, the areas detailed below 'could' be relied upon by the Police Forces under Schedule 8 of Law Enforcement Processing to capture and share with partner agencies. The conditions for sensitive processing in Schedule 8 of the Act are:

- *necessary for judicial and statutory purposes – for reasons of substantial public interest;
The sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities.*
- *necessary for the administration of justice
The sensitive processing must be necessary for the administration of justice, or the exercise of a function conferred 'on a person' by enactment. This covers a constable and other competent authorities.*
- *necessary to protect the vital interests of the data subject or another individual
This condition only applies in cases of life or death.*
- *necessary for the safeguarding of children and of individuals at risk
This condition is met in cases where consent is not appropriate because the individual is under 18 or at risk, but the processing is necessary for reasons of substantial public interest, and is to protect them from harm or to protect their well-being.*
- *personal data already in the public domain (manifestly made public)
This condition applies if the data subject has deliberately made the information public.*
- *necessary for legal claims
This condition is met if the processing is necessary for the establishment, exercise or defence of a legal claim.*
- *necessary for when a court acts in its judicial capacity
This condition is met if the processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity.*
- *necessary for the purpose of preventing fraud
This condition is used when processing is necessary for the purposes of preventing fraud. Where sharing with organisations that do not fall within the definition of a competent authority, the full lawful basis for the processing will be outlined in the Information Sharing Agreement (ISA).*
- *necessary for archiving, research or statistical purposes
This is used when processing is necessary for archiving in the public interest; for scientific or historical research purposes, or for statistical purposes.*

Accountability principle

- i. Do we maintain appropriate documentation of our processing activities?
 - *Surrey Police and Sussex Police detail all information in its Record Of Processing Activities and multiple Privacy Notices, the latter are available to the public under the FOI on the Internet.*
 - *All reasons, lawful basis, legislation and specifics of content shared are detailed in our ISA templates.*
- ii. Do we have appropriate data protection policies?
 - *1187 Information Management Policy (Surrey and Sussex)*
 - *1181 Subject Access Requests Policy (Surrey and Sussex)*
 - *1180 Data Protection Breach Policy (Surrey and Sussex)*
- iii. Do we keep logs in accordance with our obligations under section 62?
 - *Depending on the Department, logs / audits of all changes and updates to personal information are retained in line with the joint Force Retention Schedule.*
 - *All information shared, whether verbally or for evidential purposes are recorded. If the Data Protection (DPA2) form is used, the new process is for this to be saved in Niche to enable a full audit.*
 - *Details of all internal MoPI audits are retained (using URN not personal details).*
 - *All Rights to Rectification / Rights to be Forgotten are logged with Information Management and any changes to records are noted on Niche where relevant (as this can be disclosed on Rights of Access requests).*

Principle (a): lawfulness and fairness

- i. If the processing is relying on a Schedule 8 condition, is the processing strictly necessary for the identified LE purposes?
 - *This is covered on the Force Privacy Notices and also referenced in the ISA template, the relevant section is completed by Information Management (IM) to ensure the lawful process for sharing personal and special category data (including for Law Enforcement Purposes) are recorded for audit.*
- ii. If we are relying on consent for processing, are we satisfied that the consent is valid?
 - *Yes, consent is used as last resort, but if used is always full and explicit consent and all documentation is proof read by the IM Dept. to ensure the consent is relevant, not excessive and retained. All documentation is also reviewed to ensure it is compliant and all relevant rights for the participant are clear and relevant to the target audience.*
- iii. Do we make appropriate privacy information available with respect to the sensitive data?
 - *Privacy Notices:*
 - <https://www.sussex.police.uk/hyg/fpnsussex/privacy-notice/>
 - <https://www.surrey.police.uk/hyg/fpnsurrey/privacy-notice/>

Principle (b): purpose limitation

- i. Have we clearly identified our LE purpose(s) for processing as outlined in section 31?
 - *The specific reason for each item is reviewed on the asset register.*
- ii. Are our purposes for LE processing specified, explicit and legitimate?
 - *Yes, this is covered in the ISA when we share data*
 - *This is covered in the DPIA to ensure we are correctly recording the data*
 - *Privacy Notices:*
 - <https://www.sussex.police.uk/hyg/fpnsussex/privacy-notice/>
 - <https://www.surrey.police.uk/hyg/fpnsurrey/privacy-notice/>
- 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?
 - *IM attends the change meetings where new systems are assessed, at this stage the Force intention for the data will be reviewed to ensure it is still compliant with the original purpose for which it was collected.*
 - *IM has ensured Data Protection principles are embedded in all training, not just the specific UK Data Protection Legislation training. This ensures teams are aware of the processing of the information they hold and to contact IM if they have any queries.*
 - *Guidance and frequently asked questions are published on the Force Intranet to aid with all Data Protection related concerns.*
- 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 UK GDPR and DPA 2018?
 - *IM attends the change meetings where new systems are assessed, at this stage the Force intention for the data will be reviewed to ensure it is still compliant with the original purpose for which it was collected.*
 - *This is covered on the ISA template, the relevant section is completed by Information Management (IM) to ensure the lawful process for sharing personal and special category data (including for Law Enforcement Purposes) are recorded for audit.*

Principle (c): data minimisation

- i. Are we satisfied that we only collect sensitive data we actually need for our specified purposes and that it is proportionate?
 - *Information Management advise on the importance of this for Part 2 and Part 3 activities.*
 - *As an additional protective measure, a Force Retention Schedule exists to enable manual reviews on RRD.*
- ii. Are we satisfied that we have sufficient sensitive data to properly fulfil those purposes?
 - *Surrey Police and Sussex Police collect only necessary information for Part 2 and Part 3 activities.*
- iii. Do we periodically review this particular sensitive data, and delete anything we don't need?
 - *All data is held in line with retention schedule, this is also reviewed when we complete the Asset Register and annual returns.*
 - *There is a decommissioning process for legacy data which ensures old information is in the process of being deleted to ensure compliance.*

Principle (d): 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?
 - *The Data Compliance Team (DCT) in Sussex and Data Quality (DQ) in Surrey regularly monitor new entries on the Niche system and make the necessary amendments / merges to cleanse the data.*
 - *The Force Research Bureau and Data Bureau regularly monitor new entries on the Police National Computer (PNC) and Niche system and make the necessary amendments / merges to cleanse the data.*
 - *Surrey Police and Sussex Police obtain extracts from the Police National Database (PND) Dashboard and / or Niche which highlight duplicates and potential errors. This is passed back to the DCT / DQ Teams to amend to enable cleansed data in Niche which then feeds PND, Data Warehouse, Disclosure and Barring Service, etc.*
 - *Amendments are regularly made following a Rights of Rectification request, as alleged inaccuracies are flagged by the applicant which triggers an Information Management review.*
- ii. Do we distinguish between sensitive personal data based on facts and sensitive personal data based on personal assessments (opinion)?
 - *Data collected for employment / vetting purposes is clearly identified on the system holding it.*
 - *Surrey Police and Sussex Police use Niche for Crime and Intel, data collected is clearly identified on here and all Intel is graded using 3*5*2 (Source, Intelligence, Handling).*
- 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)?
 - *Surrey Police and Sussex Police use Niche for Crime and Intel processing, the system clearly distinguishes between personal data for law enforcement purposes.*
 - *There is a clear distinction between personal data relating to different categories of data subject, such as;*
 - (a) *persons suspected of having committed or being about to commit a criminal offence;*
 - (b) *persons convicted of a criminal offence;*
 - (c) *persons who are or may be victims of a criminal offence;*
 - (d) *witnesses or other persons with information about offences.*
 - *Through use of Niche for collection and storage of the information, ISA to record who we share with and why. DPA2 forms to record what has been shared, Surrey Police and Sussex Police ensure the accuracy on the quality of the data.*

Principle (e): 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?
 - *All data is held in line with retention schedule, this is also reviewed when we complete the Asset Register and annual returns.*
 - *There is a decommissioning process for legacy data which ensures old information is in the process of being deleted to ensure compliance.*
- ii. Have we established appropriate time limits for the periodic review of the need for the continued storage of this sensitive personal data?
 - *All data is held in line with retention schedule, this is also reviewed when we complete the Asset Register and annual returns.*
 - *There is a decommissioning process for legacy data which ensures old information is in the process of being deleted to ensure compliance.*

Principle (f): integrity and confidentiality (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?
 - *Both Information Management and Information Security are involved in the change meetings process for all new projects, this ensures privacy by design (Data Protection Impact Assessments – DPIA) and also all the necessary checks for information security, including penetration testing and ISO assurance.*
- 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?
 - *1192 Security Framework Policy (Surrey and Sussex)*
 - *722 SE Region Information Security Policy (Surrey and Sussex)*
 - *The above are regularly reviewed and tested by the Information Security team across both Forces*
- iii. Have we put other technical measures or controls in place because of the circumstances and the type of sensitive data we are processing?
 - *Both Information Management and Information Security are involved in the change meetings process for all new projects, this ensures privacy by design and also all the necessary checks for information security, including PEN Test and ISO assurance.*
 - *Surrey Police and Sussex Police have a thorough breach reporting process for Information Management, Information Security and Information Technology to ensure all losses of physical assets and data are recorded and reviewed within the ICO time frames. This is done electronically using the Security and Breach Reporting (SaBR) tool which generates an email to the respective Department with all details relating to the breach.*

Artificial Intelligence

- *Sussex Police and Surrey Police may use Artificial Intelligence (AI) technologies to support law enforcement processing, such as for the purposes of the prevention, detection, investigation and prosecution of criminal offences. We may also use AI technologies for administrative processing of staff details or in the case of locating Missing Persons.*
- *All processing of law enforcement data using AI is conducted in accordance with Part 3 of the Data Protection Act 2018 whereas processing for missing persons or human resource purposes will fall under the UK GDPR.*
- *All processing using AI technologies will be subject to stringent governance processes to ensure personal, special, sensitive and criminal data is handled lawfully, fairly, and transparently. The Force Privacy Notice for our use of AI technology can be found here.*

Retention and erasure policies

- *Asset Register:*
<http://surrey.shdc.police.uk/GDPR/Assets/2018%20Audit/Asset%20Register%20%20Master%202019.xls?Web=1>
- *Retention Policy:*
<http://informationhub.shdc.police.uk/layouts/15/WopiFrame2.aspx?sourcedoc=/Documents/Surrey%20Police%20and%20Sussex%20Police%20Retention%20Schedule.xlsx&action=default&DefaultItemOpen=1>

APD review date

- *Reviewed 24/10/2025*