

Appropriate Policy Document

Guidance for Completion

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document demonstrates the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles. In particular, it outlines our retention policies with respect to this data. (See Schedule 1 Part 4).

You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However, if you rely on one of these conditions, your general record of processing activities under UK GDPR Article 30 must include:

- (a) the condition which is relied upon*
- (b) how the processing satisfies Article 6 of the UK GDPR (lawfulness of processing); and*
- (c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.*

The APD therefore complements your general record of processing under Article 30 of the UK GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

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. See Schedule 1 Part 4 paragraph 40.

You should read this document alongside our [Guide to the UK GDPR](#).

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*
- *licenses or permits held (e.g. driving licenses 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.

Schedule 1 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.*

As Police, we 'could' be relied upon by the Police Forces under Schedule 1 of the [Data Protection Act](#) to capture both operational and administrative / employment data as well as further sharing with partner agencies. For full details of Part 3 processing under the Law Enforcement Directive, please see 'Appropriate Policy Document – Law Enforcement'.

Part 1 Processing: Conditions relating to employment, health and research etc

- *Employment, social security and social protection*
- *Health or social care purposes*
- *Public health*
- *Research*

Part 2 Processing: Substantial public interest conditions

- *Statutory etc and government purposes*
- *Administration of justice and parliamentary purposes*
- *Equality of opportunity or treatment*
- *Racial and ethnic diversity at senior levels of organisations*
- *Preventing or detecting unlawful acts*
- *Protecting the public against dishonesty etc*
- *Journalism etc in connection with unlawful acts and dishonesty etc*
- *Preventing fraud*
- *Support for individuals with a particular disability or medical condition*
- *Counselling*
- *Safeguarding of children and of individuals at risk*
- *Safeguarding of economic well-being of certain individuals*
- *Insurance*
- *Political parties*
- *Elected representatives responding to requests*
- *Disclosure to elected representatives*
- *Publication of legal judgments*

Part 3 Processing: Additional conditions relating to criminal convictions etc

- *Consent*
- *Protecting individual's vital interests*
- *Processing by not-for-profit bodies*
- *Personal data in the public domain*
- *Legal claims*
- *Judicial acts*
- *Administration of accounts used in commission of indecency offences involving children*
- *Extension of conditions in Part 2 of this Schedule referring to substantial public interest*
- *Extension of insurance conditions*

Privacy Notices:

<https://www.sussex.police.uk/hyg/fpnsussex/privacy-notice/>

<https://www.surrey.police.uk/hyg/fpnsurrey/privacy-notice/>

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 carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests?
 - *Yes – Information Governance is involved at all stages of change planning. This allows for compliance reviews of contracts, project plans and the completion of DPIA as required to ensure privacy by design. It also allows for involvement from Information Security to ensure the technical solution is secure.*

Principle (a): lawfulness, fairness and transparency

See general [checklist](#) for Lawfulness, fairness and transparency.

- i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data?
 - *Surrey Police and Sussex Police details 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 make appropriate privacy information available with respect to the SC/CO data?
 - *Yes – Surrey Police and Sussex Police details 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.*
- iii. Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use?
 - *Yes – Surrey Police and Sussex Police details 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.*

Principle (b): purpose limitation

See general [checklist](#) for purpose limitation.

- i. Have we clearly identified our purpose(s) for processing the SC/CO data?
 - *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/>
- ii. Have we included appropriate details of these purposes in our privacy information for individuals?
 - *Yes – Surrey Police and Sussex Police details 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.*

- iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?
 - *Yes – this decision is made based on consultation with Information Management or the DPO.*

Principle (c): data minimisation

See general [checklist](#) for Data minimisation.

- i. Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes?
 - *Yes, 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 retention.*
- ii. Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes?
 - *Yes – we collect all the necessary information for Part 2 and Part 3 activities.*
- iii. Do we periodically review this particular SC/CO 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*
 - *Annual weeding of paper files*

Principle (d): accuracy

See general [checklist](#) for Accuracy.

- i. Do we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data?
 - *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 have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary?
 - *This will be in line with the Retention Schedule or in some systems, they have automatic Review, Retain or Delete (RRD).*
- iii. Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification?
 - *Amendments are regularly made following a Rights of Rectification request, as alleged inaccuracies are flagged by the applicant which triggers an Information Management review.*
 - *The Information Management team operate processes and requests form for Rights to Rectification / Rights to be Forgotten:*

Principle (e): storage limitation

See general [checklist](#) for Storage limitation.

- i. Do we carefully consider how long we keep the SC/CO data 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.*
 - *Annual weeding of paper files.*
- ii. Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it?
 - *Both Surrey Police and Sussex Police rely on the joint Retention Schedule and Asset Register. This covers both automated and manual deletion of data that is past its retention date.*
 - *There is a new Decommissioning Process that has been implemented to assess and record all decisions to either archive or dispose of legacy data systems.*
 - *Both Surrey Police and Sussex Police have a Management of Police Information (MoPI) team that act as business expert for advice and storage, both teams also play a vital role in the compliance with retention of paper Crime files.*
- iii. Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?
 - *There is a new Decommissioning Process that has been implemented post GDPR to assess and record all decisions to either archive or dispose of legacy data systems.*
 - *Crime files are held in line with the MoPI grade of the offence.*
 - *Clear guidance has been shared with the respective Departments and individuals who produce and share statistical data to ensure that they only share anonymised or pseudonymised data.*

Principle (f): integrity and confidentiality (security)

See general [checklist](#) for 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 SC/CO 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 SC/CO 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*