Safeguards for Sensitive Processing Policy

Purpose:	This policy sets out the safeguards that data subjects may expect when the Joint Controllers are engaged in 'Sensitive Processing'
Scope:	This policy applies to the processing described within the Joint Controllership Agreement (JCA) between the organisations and Agencies named within Schedule 1 to this document
Effective Date	8th June 2026
Decommissioned date	
Deletion date[1].	

Joint Controllership of the Asset Recovery Dataset - Sensitive processing for law enforcement purposes

28 August 2025

[1] *N.B. This must be retained for six months beyond the decommissioned date. Sch.1 Part 4 Sec 40(1) DPA18*

Overview

This Appropriate Policy Document (APD) relates to the sensitive processing of personal data within the Asset Recovery Dataset (the Dataset) as described within the Joint Controllership Agreement (JCA). The Joint Controllers are listed in Schedule 1 to this APD.

This APD outlines our sensitive processing on the Dataset for law enforcement purposes and explains:

1. Our procedures for securing compliance with the law enforcement data protection principles;
2. Our policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

The Joint Controllers' statutory functions include detecting and deterring Serious and Organised Criminality. They do this through the exercise of their powers in the Proceeds of Crime Act of 2002 (POCA), which allows for the restraint and recovery of assets linked to criminality using both criminal and civil proceedings.

Part 3 of the Data Protection Act 2018 (DPA18) applies to the processing of personal data by "competent authorities" for the "law enforcement purposes".

The Joint Controllers are "competent authorities" for the purpose of processing Dataset personal data because they are either:

- listed in Schedule 7 DPA or,
- if not, they have "*statutory functions for any of the law enforcement purposes*" pursuant to Section 30(1)(b) of the DPA18.

The "law enforcement purposes" are set out at section 31 DPA18. These are the are 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.

Where any controller who is a party to the JCA processes special categories of data which is not for the primary purpose of law enforcement, information may be found about that processing by reference to that controller's privacy information and policy documents.

Sensitive Processing

Part 3 of the DPA 2018 outlines the requirement for an APD to be in place when processing sensitive personal data for law enforcement purposes.

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

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

Description of data processed

We carry out sensitive processing for law enforcement purposes in three key areas:

1. Criminal investigations
2. Intelligence
3. Financial recovery

We carry out sensitive processing of all of the categories of data defined in Sec. 35(8) of the DPA18, save that we do not process genetic data, or biometric data for the purpose of uniquely identifying an individual.

Schedule 8 conditions for processing

We carry out sensitive processing under section 35(3) DPA 2018 only where it is strictly necessary for the law enforcement purposes and it meets one of the conditions in schedule 8 of the DPA 2018.

The relevant schedule 8 conditions for our processing are Schedule 8 paragraphs:

- 1 Statutory Purposes,
- 2 Administration of Justice ,
- 6 Legal Claims,
- 7 Judicial Acts, and
- 9 Archiving etc.

Procedures for ensuring compliance with the principles

Accountability principle

Appropriate technical and organisational measures have been implemented to demonstrate the requirements of accountability. These include:

- Each of the controllers individually appointing a data protection officer who reports directly to the highest management level of that organisation.
- Adopting a 'data protection by design and default' approach to processing activities. This means that before any new or modified processing takes place, compliance with the principles of the DPA18 are embedded into the design, e.g. setting rules about who can have access to data; and by default; e.g. implementing technical security measures so

that only a person with an appropriate role can access the data being protected (Role Based Access).
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies at an organisational and agency level as well as policies which collectively regulate processing of the Dataset which is under joint control.
- Ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (1): lawfulness and fairness

Processing for law enforcement must be lawful and fair. Sensitive processing is only permissible if it is:

- based on the consent of the data subject - section 35(4); or
- is strictly necessary for the law enforcement purpose and is based on a Schedule 8 condition - section 35(5).

Our processing of sensitive data for law enforcement purposes satisfies the first Schedule 8 condition that it is necessary for the exercise of functions conferred on the Joint Controllers by legislation (including the Proceeds of Crime Act 2002 – "POCA") to recover assets for criminal purposes, recover the proceeds of crime and disrupt and deter criminality. Such activity is necessary for reasons of substantial public interest. We together take action to prevent; investigate; detect; and prosecute offences contained in POCA and the criminal offences giving rise to the proceeds of crime. The actions we take are specifically within the Governmental strategy addressing Serious and Organised Crime and the POCA legislation has been specifically enacted and further amended for these purposes. In this regard, the processing of personal data for these purposes is for reasons of substantial public interest.

Principle (2): purpose limitation

We may process personal data collected for one of these purposes (whether by us or another controller), for any of the other law enforcement purposes providing the processing is necessary and proportionate for that purpose.

We will only use data collected for a law enforcement purpose for purposes other than law enforcement where we are authorised by law to do so.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

Principle (3): data minimisation

The information we process is necessary for and proportionate to our purposes. It is processed specifically to enable us to meet our stated purposes for processing. We explicitly do not widely harvest sensitive personal data outside of these stated parameters.

Where sensitive personal data is provided to us or obtained by us but is not relevant to our stated purposes, we will erase it.

Principle (4): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, we will document our decision.

As far as is reasonably possible we make it possible to distinguish personal data based on facts and personal data based on opinion. This is achieved through the way fields in processing systems are described and by annotations to records, however there may be circumstances where identification is not possible.

Likewise, we seek to make it possible to identify personal data relating to where possible to different categories of data subject where it is relevant to do so and in line with the overarching purposes of the processing e.g.:

- People suspected of committing an offence or being about to commit an offence
- People convicted of a criminal offence
- Known or suspected victims of a criminal offence
- Witnesses or other people with information about offences
- Persons who are identified as having assets within the jurisdiction of POCA which the legislation has allowed or would potentially allow to be recovered from them
- Persons with an innocent interest in a potentially recoverable or recovered asset within the scope of POCA

This is achieved through the way fields in processing systems are described and where necessary, by annotations to records. If the status of a data subject changes, then we will amend the record and outline the reason for the change e.g. should a suspect be convicted of the offence, their status will be updated in our records.

We take reasonable steps to ensure that personal data, which is inaccurate, incomplete or out of date is not transmitted or made available for any of the law enforcement purposes. We do this by verifying any data before sending it externally. We also provide the recipient with the necessary information we hold to assess the accuracy, completeness and reliability of the data.

If we discover, after transmission that the data was incorrect or should not have been transmitted, we will tell the recipient as soon as possible.

We record our decision to make personal data available for any of the law enforcement purposes.

Principle (5): storage limitation

We have a retention schedule agreed between the Joint Controllers for data processed within the scope of the JCA and retain information processed for the purposes of law enforcement in accordance with Schedule 2 to this document unless there is a legitimate reason to retain it for longer.

Principle (6): security

Electronic information is processed within our secure network. Hard copy information is processed within our secure premises. Where it is necessary for us to share information with third parties, we consider the technical or organisational security measures they have in place before allowing access or transmitting data.

Electronic and hard copy information processed for the law enforcement purposes is only available to staff who carry out the processing for these purposes. Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data for law enforcement purposes allow us to erase or update personal data at any point in time. They also allow us to log the following information:

- Collection
- Alteration
- Consultation (access)
- Identity of person who accessed
- Disclosures
- Combination of records
- Erasure

Retention and erasure policies

The Joint Controllers have a retention schedule specifically dealing with the personal information processed within the scope of the JCA for law enforcement purposes. Personal information is retained in line with that schedule unless there is a legitimate reason to retain it for longer.

Our retention and erasure practices are set out in our retention schedule, which may be found at Schedule 2 to this document.

Outside of JCA scope

Information about wider processing activities carried out by the controllers in their independent capacities can be obtained direct from the respective controllers individually.

APD review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.

Schedule 1

Asset Recovery Dataset

The Joint Controllers

Purpose:	This document sets out the organisations and agencies which are identified as being Joint Controllers of the Asset Recovery Dataset. The primary source of this information is the Joint Controllership Agreement which should be relied upon as the definitive source of information
Scope:	N/A
Effective Date	8th June 2026
Decommissioned date	
Deletion date[2].	

The Joint Controllers:

1. The National Police Chiefs' Council (NPCC) **Police forces of England and Wales[3]**
2. **National Crime Agency** (NCA)
3. Secretary of State for the Home Department (the **Home Office**)
4. **HM Revenue and Customs**
5. Ministry of Justice (to include **HM Courts and Tribunals Service**)
6. **Crown Prosecutions Service** (CPS)

The Chief Officers of the Police Forces listed below are Joint Controllers under this Arrangement by virtue of having been entered into it by the authorised 'Data Protection

[2] *N.B. This must be retained for six months beyond the decommissioned date. Sch.1 Part 4 Sec 40(1) DPA18*

[3] See full list of NPCC police forces

Lead' nominated by the NPCC portfolio holder for Economic and Cyber Crime. This is consistent with the terms of the NPCC Joint Controllership Agreement (JCA) version 2, approved and adopted by the Chair of the NPCC DDaTCC on 7 June 2024.

Avon & Somerset Constabulary
Bedfordshire Police
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Cleveland Police
Cumbria Constabulary
Derbyshire Constabulary
Devon & Cornwall Police
Dorset Police
Durham Constabulary
Dyfed-Powys Police
Essex Police
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
Humberside Police
Kent Police
Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Merseyside Police
Metropolitan Police Service
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Warwickshire Police
West Mercia Police
West Midlands Police
West Yorkshire Police
Wiltshire Police

Schedule 2

Asset Recovery Dataset – Personal Data Processed for *'Data Profiling'* Retention Schedule

Purpose:	To provide clarity in respect of the retention and subsequent deletion of data which is processed pursuant to 'profiling' of The Dataset. Profiling is an exercise whereby the data is to be assessed in order to establish its qualities, e.g. completeness, accuracy and field alignment etc. .
Scope:	This Retention Schedule will apply solely for the purposes of the profiling exercise. It will be decommissioned once that processing is complete, when it will be replaced with an updated schedule detailing retention for the contemporary processing.
Effective Date	8th June 2026
Decommissioned date	
Deletion date[4].	

The Dataset will be profiled during early 2026. Three months after profiling is complete, all personal data used in that exercise will be permanently deleted.

[4] *N.B. This must be retained for six months beyond the decommissioned date. Sch.1 Part 4 Sec 40(1) DPA18*