Joint Controllership Agreement (JCA)

Made under Section 58 of the Data Protection Act 2018 (DPA)

between

The Controllers listed in Schedule 1 to this JCA

in respect of

Processing of the

Asset Recovery Dataset

Version 7

09 December 2025

1. Introduction

1.1. These Arrangements have been produced by the Joint Controllers to satisfy the obligations placed upon them by Section 58 of the DPA and Article 26 of the UK GDPR in respect of their Processing of Personal Data within the Dataset.

1.2. The arrangements set out in a transparent manner, the respective responsibilities of each Joint Controller to comply with the DPA and UK GDPR.

1.3. The parties to these arrangements as Joint Controllers for the Dataset are detailed in Schedule 1, together with any other organisation or agency which is subsequently brought within scope of this agreement as a signatory to Schedule 1.

1.4. No other persons beyond the Joint Controllers who are parties to these arrangements may act as Controllers in respect of Personal Data within the Dataset.

2. Definitions for terms used in this document

2.1. **Arrangements** – means the arrangements as set out in this document.

2.2. **Chief Officer** – means the Chief Constable or Commissioner of a UK police force.

2.3. **Competent Authority, Controller, Data Protection Principles, Data Subject, Joint Controller, Law Enforcement Purposes, Personal Data, Processing, Processor**, and **Technical and Organisational Measures** have the meanings given to them in the DPA and UK GDPR.

2.4. **Data Protection Lead** - means an individual other than a Joint Controller authorised to act on behalf of the Joint Controllers within the terms of this agreement.

2.5. **the Dataset** - means the asset recovery dataset, which is the set of personal data determined to be under the controllership of the Joint Controllers for the purposes of transfer into the ARIT system and thereafter processed for operational purposes, together with the JCD.

2.6. **DPA18** - means the Data Protection Act 2018.

2.7. **DPIA** - means Data Protection Impact Assessment

2.8. **DPO** – means Data Protection Officer.

2.9. **Erasure or Restriction of Processing Application** – means the exercise by a Data Subject of their rights under Section 47 of the DPA, or Article 17 of the UK GDPR and Article 18 of the UK GDPR.

2.10. **General Processing** – means any processing of Personal Data by the Joint Controllers other than for Law Enforcement Purposes.

2.11. **ICO** – means the Information Commissioner's Office.

2.12. **JARD data collection** - means the cumulative personal data processed within the JARD which is not subject to this JCA.

2.13. **JCD** – means the "JARD Copy Data", which are copies of data from JARD created under the direction of the Joint Controllers for the purposes of preparatory activity ahead of transition of processing to the new ARIT platform

2.14. **Joint Controllers** – means all the Controllers listed in Schedule 1.

2.15. **Lead Controller** – means the Joint Controller which takes the lead on certain matters on behalf of all the Joint Controllers. Under these Arrangements the Commissioner of the City of London Police acts in this capacity.

2.16. **National Agreements** - means Data Sharing Agreements (DSAs), Memoranda of Understanding (MoUs), Data Processing Contracts (DPCs), Joint Controllership Agreements (JCAs) where they relate to processing of Personal Data within or from the Dataset.

2.17. **NPCC** - means the National Police Chiefs' Council. This is a body formed under Section 22A of the Police Act 1996 and its membership comprises the executive level of member organisations including the Chief Officer (Chief Constable/Commissioner) which together co-ordinate the work of the police service in order to protect the public.

2.18. **Personal Data Breach** - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data subject to Joint Controllership.

2.19. **Rectification Application** – means the exercise by a Data Subject of their rights under Section 46 of the DPA or Article 16 of the UK GDPR.

2.20. **Right of Access Application** – means the exercise by a Data Subject of their rights under Section 45 of the DPA or Article 15 of the UK GDPR.

2.21. **Security Incident** – means an occurrence, suspected or confirmed, to have led to a compromise of the confidentiality, integrity or availability of the Dataset. A Personal Data Breach is an example of a Security Incident.

2.22. **UK GDPR** – means the United Kingdom General Data Protection Regulation.

2.23. A reference to a statute or statutory provision will include all subordinate legislation made from time to time under that statute or statutory provision.

2.24. A reference to writing or written includes fax and email.

2.25. Unless the context otherwise requires the reference to one gender will include a reference to all genders.

3. Description of the Dataset

3.1. The Dataset comprises of records arising from the recovery of assets (to include those which are potentially recoverable) particularly by virtue of the legislative framework provided for by the Proceeds of Crime Act 2002 (POCA) and other relevant enactments. Assets may be of any description including but not limited to cash, bank funds, cryptographic currency, property, vehicles, jewellery etc. Records will include the identity and details of the individual or company linked to the asset, together with progress of the cases through court proceedings as well as linked artefacts such as Court Orders etc.

3.2. The Dataset is generally used by the Joint Controllers for the purposes of tracking the progress of asset recovery activity across one or more organisations or agencies throughout the case lifecycle. The dataset also serves as a collection of financial intelligence which supports ongoing investigations and ensures that organisations and agencies utilising the legislation are aware of reciprocal interests in individuals and companies. The dataset enables the contributions of organisations and agencies in recovering assets to be understood such that Asset Recovery Incentivisation Scheme (ARIS) funds can be distributed appropriately.

3.3. Each of the Joint Controllers contribute Personal Data to the Dataset and this pooled data is directly accessible for use by each of the Joint Controllers for the purposes outlined above and subject to configured rules of access.

3.4. Where a JCD or subsequent JCDs is/are created and form part of the Dataset, they will explicitly not be used to serve any operational purposes unless and until transferred into ARIT as the live system. Until the JCD or JCDs is/are transferred to the live ARIT system, the sole purpose of a JCD will be linked to preparatory activity ahead of transition to the new ARIT platform. In particular, this activity will enable the data's properties and qualities to be established, including but not limited to its accuracy, completeness and alignment to fields etc.

4. Jurisdiction and limits of Joint Controllership

4.1. The Personal Data falls under Joint Controllership at a number of junctures:

- When a JCD is created by copying the JARD data collection or a subset of that collection;
- When the Joint Controllers assume control of the JARD data collection or subset of that collection for the purposes of migration into and processing within the new operational platform, ARIT;
- When either or both previous conditions are met, Personal Data falls under Joint Controllership at the point it is added to or created within the Dataset and remains under Joint Controllership until the point it is erased from the Dataset

4.2. The following processing activities fall outside of the scope of Joint Controllership and therefore under the Controllership of the requisite Controller acting in its capacity as an Independent Controller:

- Creation and processing of other Personal Data outside the Dataset that is used to inform the input of Personal Data into the Dataset
- Access and viewing of Personal Data within the operational Database.
- Creation and further processing of copies of Personal Data from the Dataset where those copies do not meet the definition of a JCD.

5. Roles

Joint Controllers

5.1. These Arrangements have been made between the independent controllers of the organisations/agencies listed in Schedule 1 when acting together as Joint Controllers for the processing of Personal Data within the Dataset in compliance with the parameters set out at 4 above.

Lead Controller

5.2. It is agreed by the signatories to this document that the Lead Controller under this arrangement shall be the National Police Chief's Council (NPCC) Lead Force for 'Economic Crime'.

5.3. As Lead Controller, they will ensure that activities necessary for Data Protection compliance for the Dataset will be undertaken on behalf of the Joint Controllers.

Data Protection Lead

5.4. The Lead Controller may delegate activities necessary for Data Protection compliance for any processing of Personal Data to another individual who is not one of the Controllers. When acting in that capacity the other individual is referred to as the Data Protection Lead.

5.5. The Data Protection Lead role should not be confused with the separate and statutory role of Data Protection Officer.

Leads for Subject Rights

5.6. Each Controller will identify a Lead for Subject Rights applications made to their organisation/agency under the DPA and/or UK GDPR.

6. Responsibilities and accountabilities

6.1. The following responsibilities and accountabilities apply in relation to Personal Data processed by the Joint Controllers within the Dataset under these Arrangements.

Joint Controllers

6.2. Each Joint Controller is jointly responsible and is jointly accountable for compliance with the DPA and UK GDPR and for ensuring compliance with these Arrangements.

6.3. Each Joint Controller will comply with any Codes of Connection or similar documents introduced for the Dataset and comply with any future standards as agreed by the Lead Controller.

6.4. Each Joint Controller will use their best endeavours to ensure the accuracy of the data submitted to the Dataset.

6.5. Each Joint Controller will ensure that the following Data Protection compliance activities take place within their respective organisation or agency in respect of the Dataset:

- Personal Data is processed in accordance with the Data Protection Principles
- Data Subject Rights are respected in accordance with Chapter 3 of Part 3 of the DPA and Chapter III of the UK GDPR
- Appropriate technical and organisational measures are implemented to ensure, and to be able to demonstrate, compliance with Data Protection legislation as per Section 56 of the DPA and Article 24 of the UK GDPR
- Data Protection by design and default is achieved as required by Section 57 of the DPA and Article 25 of the UK GDPR
- Records of Processing Activities are maintained in accordance with Section 61 of the DPA and Article 30 of the UK GDPR
- Logging requirements are met as per Section 62 of the DPA
- Data Protection Impact Assessments (DPIAs) are conducted and maintained in compliance with Section 64 of the DPA and Article 35 of the UK GDPR
- International transfers of Personal Data are compliant with Chapter 5 of Part 3 of the DPA and Chapter V of the UK GDPR.
- The terms of these Arrangements are complied with

6.6. Each Joint Controller to which the Equality Act 2010's (EA2010) Public Sector Equalities Duty (PSED) is applicable will ensure that the duty in respect of their role in 'Asset Recovery' is being met.

Lead Controller

6.7. The Lead Controller, in addition to responsibilities arising as a Joint Controller, is authorised on behalf of the Joint Controllers to:

- implement processes for the management of access to the Dataset
- add additional Controllers to these Arrangements
- implement appropriate Data Governance measures for the Dataset
- implement a Review, Retention & Disposal policy for the Dataset
- enter into Data Sharing Agreements or Memoranda of Understanding on behalf of the Joint Controllers where Personal Data is involved, subject to compliance with prevailing governance procedures which may be amended from time to time and in compliance with the law.
- appoint and oversee Processors to process Personal Data on behalf of the Joint Controllers, including the creation and signing of associated Data Processing Contracts, subject to compliance with prevailing governance procedures which may be amended from time to time and in compliance with the law
- enter into sharing arrangements where the sharing involves statistical data rather than Personal Data
- enter into Joint Controllership Agreements on behalf of the Joint Controllers, subject to such agreements complying with the law

6.8. The Lead Controller may delegate any of the compliance activities and authorised activities set out under clause 6.7 to any nominated Data Protection Lead.

6.9. The Lead Controller will fulfil the role of 'Contact Point' to data subjects as mandated by virtue of Section 58(3) of the DPA.

Data Protection Lead

6.10. Where nominated the Data Protection Lead is authorised to undertake any Data Protection compliance activities delegated from the Lead Controller under clause 6.8, or alternatively ensure that such activities are completed on their behalf.

Leads for Data Subject Rights

6.11. The Leads for Data Subject Rights act in support of the Lead Controller's responsibilities as 'Contact Point' in discharging subject rights and will operate in accord with their directions for the fulfilment of those obligations.

6.12. The Leads for Data Subject Rights must comply with these Arrangements.

7. Damages - liability

7.1. Any determination as to how potential liabilities might be met, should they arise, is out of scope of this document.

8. Data Subject Rights Applications

8.1. Schedule 2 to this JCA sets out the current mechanism by which Data Subjects may access their subject rights under this section.

9. Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR) Applications[1]

9.1. The FOIA and EIR are applicable to *most* Public Authorities and in some circumstances to bodies carrying out public functions. Leads for Data Subject Rights act as the primary points of contact for those organisations and agencies to which the Act and regulations apply. *N.B. The NCA is not a body to which the FOIA applies. Furthermore, information held by public authorities that was supplied to them directly or indirectly by the NCA or relates to the NCA is exempt information [from disclosure] for the purposes the FOIA 2000 by virtue of Sec.23 of the Act.*

9.2. Individuals wishing to exercise their rights under the Freedom of Information Act 2000/Freedom of Information (Scotland) Act 2002 and Environmental Information Regulations 2004/Environmental Information (Scotland) Regulations 2004 (EIR) should direct their request to the relevant lead for the organisation or agency in which they have an interest.

9.3. Where a request has the potential to affect another organisation or agency, the lead for Data Subject Rights should liaise with the other organisation or agency and take into consideration their views before making any response.

10. Data retention and Disposal

10.1. Each Joint Controller will only retain or process Personal Data within the Dataset for as long as is necessary in connection with the purposes it has been retained for in accordance with legislation and relevant national, local or dataset-specific guidelines/policy.

11. Security and Training

11.1. Each Joint Controller will implement and maintain appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk posed by the Processing undertaken under these Arrangements.

11.2. The Joint Controllers will keep such security measures under review and will carry out such updates as they deem to be appropriate throughout the term.

11.3. It is the responsibility of each Joint Controller to ensure that staff members are appropriately trained to handle and process data in accordance with the Technical and Organisational Measures it implements.

---

[1] Section 58 of the DPA18 does not place a requirement for FOI and EIR arrangements to be included in Joint Controller Arrangements, but these are included for completeness.

12. Information Security Incidents including Personal Data Breaches and reporting procedures

12.1. Each Joint Controller is responsible for reporting and managing any actual or suspected Information Security Incident (including Personal Data Breach) relating to data processed under these Arrangements in accordance with their own organisation/agency policy, procedure or process.

12.2. Each Joint Controller is also responsible for deciding whether any Personal Data Breach is reportable to the ICO in accordance with DPA and/or UK GDPR, and (where applicable) inform Data Subjects as required by the DPA and/or UK GDPR. Prior to any notification to the ICO and/Data Subjects they will inform the Lead Controller of the occurrence so that the latter can consider what further actions are necessary.

12.3. Where an Information Security Incident is of a nature that could affect other Joint Controllers, the Joint Controller concerned will inform the Lead Controller of the occurrence so that the latter can consider what further actions are necessary.

12.4. In the event that a Joint Controller becomes aware of any Information Security Incident (including Personal Data Breach) involving another Joint Controller they will inform that Joint Controller without undue delay.

12.5. The relevant Joint Controllers will provide reasonable assistance as is necessary to each other to facilitate the handling of any Information Security Incident (including Personal Data Breach) in an expeditious and compliant manner.

13. Review and governance arrangements

13.1. These Arrangements will remain in force until terminated by a majority number of the Joint controllers and following a review as at 13.2.

13.2. The Lead Controller will on behalf of the other Joint Controllers initiate an annual review of these Arrangements or on request of one or more of the other Joint Controllers an immediate review of the Arrangements. The Joint Controllers may decide to continue, amend or terminate the Arrangements depending on the outcome of any review.

13.3. The review set out at 13.2 will involve:

- Assessing whether the purposes of Processing are still law enforcement purposes and whether the purposes should be revised
- Assessing whether the legal framework governing data quality, retention, and Data Subjects' and individuals' rights are being complied with
- Assessing whether policies regulating the processing of personal data under the Joint Controllership are being complied with Assessing whether Personal Data Breaches have been handled in accordance with these Arrangements and the relevant legal framework

13.4. The Joint Controllers will provide reasonable assistance as is necessary to facilitate the conduct of any review in an efficient and expeditious manner.

14. Signatories

14.1. The Joint Controllers have confirmed in writing their acceptance of and commitment to comply with these arrangements by signing and dating Schedule 1.

14.2. Where a signatory to this agreement is entering into it on behalf of another Joint Controllership, they will be considered a singular entity for the purposes of this agreement

Schedule 1 to the 'Asset Recovery Dataset' JCA - Police Joint Controllers

A

Signatories to this document agree to be bound collectively to the terms of this JCA from the recorded date of entry until such time as their participation is ended in accordance with the terms established within the document.

Policing (England and Wales)
I acknowledge and accept in writing, and sign on behalf of the joint controllers in England and Wales.

Name:	Nik Adams
Post and Grade:	Deputy Chief Constable NPCC Lead for Economic and Cyber Crime on behalf of the NPCC forces of England and Wales
Signature:	
Date:	Click or tap to enter a date.

National Crime Agency
I acknowledge and accept in writing, and sign on behalf of the Director General of the National Crime Agency.

Name:	Click or tap here to enter text.
Post and Grade:	Click or tap here to enter text.
Signature:	
Date:	Click or tap to enter a date.

Home Office
I acknowledge and accept in writing, and sign on behalf of the Secretary of State for the Home Department.

Name:	Click or tap here to enter text.
Post and Grade:	Click or tap here to enter text.
Signature:	
Date:	Click or tap to enter a date.

HMCTS

I acknowledge and accept in writing, and sign on behalf of the Ministry of Justice.

Name:	Click or tap here to enter text.
Post and Grade:	Click or tap here to enter text.
Signature:	
Date:	Click or tap to enter a date.

HM Revenue and Customs

I acknowledge and accept in writing, and sign on behalf of HM Revenue and Customs.

Name:	Click or tap here to enter text.
Post and Grade:	Click or tap here to enter text.
Signature:	
Date:	Click or tap to enter a date.

CPS

I acknowledge and accept in writing, and sign on behalf of the CPS.

Name:	Click or tap here to enter text.
Post and Grade:	Click or tap here to enter text.
Signature:	
Date:	Click or tap to enter a date.

B

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 Lead' nominated by the NPCC portfolio holder for Economic and Cyber Crime. This is consistent with the terms of the 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 to the 'Asset Recovery Dataset' JCA – Data Subject Rights

The Dataset:	Asset Recovery Dataset
Description:	Jard Copy Data (JCD)
Valid - Date From:	
Lead Organisation/Agency (Controller) for Data Subject Rights:	City of London Police (CoLP)
Retention Period for this schedule:	12 months after either: • This schedule is updated and replaced; or, • The processing of personal data is discontinued and the data is deleted.
End Date:	

Subject Rights

Personal data held within the JCD(s) will be held for a limited period allied to the purposes described in brief within the Joint Controllership Agreement. Once those purposes have been fulfilled, the data will be deleted in accordance with the retention schedule.

During the lifetime of a JCD, data subjects may exercise their Subject Rights, these being the:

- Right of Access – Sec. 45 DPA18
- Right of Rectification – Sec. 46 DPA18
- Right to Erasure or Restriction of Processing – Sec. 47 DPA18

As a Data Subject, should you wish to access these rights, you are encouraged to make your application as set out below.

1. Making a Request

You are encouraged to submit your Subject Rights request directly to the '**City of London Police'** as **lead controller** and **'contact point'** for Subject Rights:

Email: data.protection@cityoflondon.police.uk
Postal: Information Access Team, City of London Police, 182 Bishopsgate, London EC2M 4NP

You may also make your request to any other controller a party to this Joint Controllership arrangements in which case that organisation will:

1. Acknowledge receipt of the request.
2. Forward it securely to the CoLP Information Access Team within 5 working days of receipt.

3. Notify the data subject that their request has been referred to the lead controller for coordination.

2. Verification of Identity

Before your request is considered, the CoLP Information Access Team must verify your identity.

This may include requesting:

- Proof of ID (e.g., passport, driving licence)
- Proof of address (e.g., utility bill, council tax statement)

If the request is made on behalf of another person, evidence of authority (e.g., signed consent or power of attorney) is required.

3. Acknowledgement and Initial Assessment

The CoLP Information Access Team will:

- Acknowledge the request within 5 working days of receiving the request from you or, where you made the request via another controller, within 5 working days of receiving your request from them
- Determine whether the request falls within the Asset Recovery dataset
- Notify all potentially relevant controllers.

4. Further Information

You are advised that further information in regard to pursuing your Subject Rights and applicable time scales etc. may be obtained from the CoLP direct by accessing the following link: https://www.cityoflondon.police.uk/advice/advice-and-information/data-pro/data-protection/