



**Joint Controllership Agreement (JCA)**  
**Made under Section 58 of the Data Protection Act 2018**  
**(DPA) and Article 26 of the United Kingdom General Data**  
**Protection Regulation (UK GDPR)**

**between**

**The Chief Officers of the police forces**  
**listed in Schedule 1 of this JCA**

**for**

**the Processing of Personal Data relating**  
**to National Police Chiefs' Council**  
**functions and associated matters**

**Version 2.0**

**Endorsed by the National Policing Data & Analytics Board**  
**on 12th December 2023**

**Approved and adopted by the Chair of the**  
**NPCC Digital, Data and Technology Co-ordination Committee**  
**on 7<sup>th</sup> June 2024**

This document is suitable for dissemination into the public domain

## 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 Joint Processing of Personal Data. They were first issued on 7<sup>th</sup> December 2022 and this version replaces that original version.
- 1.2. The Arrangements set out in a transparent manner, the respective responsibilities of each Controller to comply with the DPA and UK GDPR.
- 1.3. These Arrangements apply to the processing of Personal Data carried out by a Competent Authority for Law Enforcement Purposes in accordance with Part 3 of the DPA (hereinafter referred to as a “Law Enforcement Processing”) and for any other purposes (hereinafter referred to as a “General Processing”).
- 1.4. In accordance with clause 3.2 below, these Arrangements primarily relate to the Joint Controllorship of Personal Data undertaken pursuant to the discharge of the functions of the NPCC as set out in the [NPCC Collaboration Agreement made under s22A Police Act 1996](#) (NPCC 22A) and more particularly those functions set out in Clause 7 thereof, and describe the processes referred to in Clause 25 thereof.
- 1.5. For administrative convenience this document also covers the following matters associated with Joint Controllorship:
  - Data Sharing (section 11)
  - Data Governance of National Datasets (section 12)
  - Data Protection Governance of National Units outside scope of these Arrangements (section 13)
  - Use of Agents to enter into Data Processing Contracts where Personal Data is not subject to Joint Controllorship by the NPCC Chief Officers (section 14)
- 1.6. Each Chief Officer remains responsible for their Processing of Personal Data for purposes beyond the scope of the NPCC 22A.
- 1.7. Schedule 1 lists the Controllers entering into this Arrangement. Schedule 2 summarises the roles, designations and responsibilities described in greater detail in sections 3 and 4. Schedule 3 sets out the process of approval of National Agreements.

## 2. Definitions for terms used in this document

- 2.1. **Agent** – means a Joint Controller authorised by the NPCC Chief Officers to enter into Data Processing Contracts on their behalf where the processing is not subject to NPCC Joint Controllorship.
- 2.2. **Arrangements** – means the arrangements as set out in this Joint Controller Agreement.
- 2.3. **CCC** – means the Chief Constables’ Council.
- 2.4. **Chief Officer** – means the Chief Constable or Commissioner of a UK police force.
- 2.5. **Chief Constables’ Council** – means the key decision-making body of the NPCC where operationally independent Chief Officers may agree common approaches and the national Co-ordination of the police service.
- 2.6. **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. In the case of 'Joint Controllers' this means the Chief Officers of the police forces listed in Schedule 1.

- 2.7. **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.
- 2.8. **Data Protection Principles** – means [Chapter 2 of Part 3](#) of the DPA and [Chapter II](#) of the UK GDPR.
- 2.9. **DDaT** – means Digital, Data and Technology.
- 2.10. **DPA** – means the [Data Protection Act 2018](#).
- 2.11. **DPO** – means Data Protection Officer.
- 2.12. **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](#).
- 2.13. **General Processing** – means any processing of Personal Data by the Joint Controllers other than for Law Enforcement Purposes.
- 2.14. **ICO** – means Information Commissioner's Office.
- 2.15. **Joint Controllers** – see under 3.1
- 2.16. **Joint Processing** – means any processing of Personal Data by the Joint Controllers under these Arrangements.
- 2.17. **Lead Controller** – means a Joint Controller authorised to act on behalf of the Joint Controllers within the terms of this agreement.
- 2.18. **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 under the NPCC.
- 2.19. **National Database** – means a database and its related IT infrastructure which is identified as such by the DDaT Co-ordination Committee.
- 2.20. **National Unit** – means a policing capability whose scope, purposes, and manner of delivery have been broadly agreed by multiple Chief Officers for whom that capability is provided.
- 2.21. **NPCC** – means the National Police Chiefs' Council. This is a body formed under section 22A of the Police Act 1996, consisting of Chief Officers which co-ordinates the work of the police service in order to protect the public.
- 2.22. **NPCC Chief Officer** - means the Chief Constable or Commissioner of the 46 UK police forces listed in Schedule 1.
- 2.23. **NPCC Controllers** – means the NPCC Chief Officers party to these Arrangements when not acting as Joint Controllers.
- 2.24. **NPCC Co-ordination Committee** – means a committee, led by a Chief Officer, which leads on a broad area of policing business and reports to the Chief Constables' Council. Each Co-ordination Committee may be supported by NPCC Portfolios, Sub-Committees, Working Groups, and other sub-structures.
- 2.25. **NPCC Portfolio** – means a specific area of policing business led by a Portfolio Lead who reports to a parent Co-ordination Committee.
- 2.26. **NPCC Portfolio Lead** – means the individual designated to lead an NPCC Portfolio.
- 2.27. **NPCC Programme** – means a team leading a distinct body of work which is identified as necessary for a period of time by Chief Constables' Council, to respond to an

emerging and significant policing problem which may reach across multiple NPCC Co-ordination Committee areas.

- 2.28. **NPCC 22A** – means the NPCC Collaboration Agreement made under s22A Police Act 1996 (as amended).
- 2.29. **NPCC Working Group** – means a part of the sub-structure of an NPCC Co-ordination Committee and Portfolio which is tasked with managing a policing issue.
- 2.30. **NPFDU** – means the National Police Freedom of Information and Data Protection Unit.
- 2.31. **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.
- 2.32. **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](#).
- 2.33. **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](#).
- 2.34. **Section 22A Body** – means a body established in accordance with a collaboration agreement under section 22A of the Police Act 1996.
- 2.35. **UK GDPR** – means the [United Kingdom General Data Protection Regulation](#).
- 2.36. A reference to a statute or statutory provision will include all subordinate legislation made from time to time under that statute or statutory provision.
- 2.37. A reference to writing or written includes fax and email.
- 2.38. Unless the context otherwise requires the reference to one gender will include a reference to all genders.

### 3. Roles

#### Joint Controllers

- 3.1. These Arrangements have been made between the Chief Officers of the police forces listed in Schedule 1 when acting together as Joint Controllers.
- 3.2. Those Chief Officers are Joint Controllers when processing Personal Data for the purposes and exercise of the functions of the NPCC arising from the NPCC 22A.<sup>1</sup>

#### Lead Controllers

- 3.3. Within that context the Joint Controllers have determined that the Chair of each Co-ordination Committee is the Lead Controller for Personal Data processed by their Co-ordination Committee and any NPCC Portfolios, Sub-Committees, Working Groups and other sub-structures subordinate to their Co-ordination Committee.
- 3.4. The leads of each National Unit and NPCC Programme are either a Lead Controller (if they are a Chief Officer) or are referred to as a Data Protection Lead for the processing of Personal Data by their entity.

#### Data Protection Leads

---

<sup>1</sup> It is accepted that any other Section 22A Body beyond the NPCC could, in accordance with its arrangements under section 22A of the Police Act 1996, be a Controller with regards to the Processing activities undertaken to discharge its functions, solely or jointly with the Chief Officers, including (if so designated) in its arrangements) as Lead Controller.

- 3.5. Lead Controllers may delegate to the leads of their subordinate NPCC Portfolios, Sub-Committees, Working Groups and any other sub-structures activities necessary for Data Protection compliance for any processing of Personal Data by those subordinate entities. When acting in that capacity those leads are referred to as Data Protection Leads.
- 3.6. The Joint Controllers have determined that the NPCC Chair is the Data Protection Lead for Personal Data processed for the purposes of the administration of Chief Constables' Council and by the NPCC Strategic Hub.

#### **Lead for Data Subject Rights**

- 3.7. The Lead for Data Subjects Rights is the National Police Freedom of Information and Data Protection Unit (NPFDU).

#### **NPCC Senior Information Risk Owner (SIRO)**

- 3.8. DDaT Co-ordination Committee shall allocate an individual to act as SIRO for information including Personal Data and other information processed under these Arrangements not falling under the scope of the National SIRO responsibilities.

#### **Information Asset Owners (IAOs)**

- 3.9. Chairs of Co-ordination Committees are IAOs for information, including Personal Data, processed by their Co-ordination Committee and any subordinate NPCC Portfolio, Sub-Committee, Working Group or sub-structures.
- 3.10. National Unit leads and NPCC Programme leads are IAOs for information, including Personal Data, processed by their entities.
- 3.11. The NPCC Strategic Hub Lead is the IAO for information including Personal Data processed for the purposes of the administration of Chief Constables' Council and by the NPCC Strategic Hub.

## **4. Responsibilities and Accountabilities**

- 4.1. The following responsibilities and accountabilities apply in relation to Personal Data processed by the Joint Controllers for the purposes and exercise of the functions of the NPCC arising from the NPCC 22A under these Arrangements.

#### **Joint Controllers**

- 4.2. 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.
- 4.3. The Joint Controllers have delegated certain Data Protection compliance activities to the Lead Controllers as set out below.

#### **Lead Controllers**

- 4.4. The Lead Controllers must ensure that the following Data Protection compliance activities take place within their Co-ordination Committee and its sub-structures:
  - 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](#) (see Section 8)
  - 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](#)
  - Where applicable, 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
- 4.5. Where a DPIA identifies that processing is likely to result in a high risk to the rights and freedoms of Data Subjects they must bring this to the attention of the Chair of the DDaT Co-ordination Committee, who will determine whether the risk is acceptable or will escalate that decision to CCC. The NPCC DPO will undertake any prior consultation with the ICO if required in accordance with [Section 65 of the DPA](#) and [Article 35 of the UK GDPR](#).
- 4.6. The Lead Controllers:
- are authorised to enter into Data Sharing Agreements or Memoranda of Understanding on behalf of the Joint Controllers, subject to compliance with the procedure set out in Schedule 3 and compliance with the law
  - are authorised to 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 the procedure set out in Schedule 3 and compliance with the law
  - are authorised to enter into Joint Controllership Agreements on behalf of the Joint Controllers, subject to such agreements complying with the law
  - may obtain necessary Data Protection advice and support from their home force or from the NPCC DPO, or from another external source
- 4.7. The Lead Controllers may delegate any of the compliance activities and authorised activities set out under clauses 4.4 to 4.6 to their sub-ordinate Data Protection Leads.

### **Data Protection Leads**

- 4.8. The Data Protection Leads are authorised to undertake any Data Protection compliance activities delegated from the Lead Controller under clause 4.7, or alternatively ensure that such activities are completed on their behalf.
- 4.9. Where a Data Protection Lead does not sit within the sub-structure of a Co-ordination Committee, they have delegated authority and responsibility to undertake the Data Protection compliance and other activities set out under clauses 4.4 to 4.6 of these Arrangements.
- 4.10. The Chair of the NPCC is authorised on behalf of NPCC to enter into Data Sharing Agreements or Memoranda of Understanding on behalf of the NPCC where there is no obvious Lead Controller or Data Protection Lead to undertake that task. They are also authorised to undertake the Data Protection compliance and other activities set out under clauses 4.4 to 4.6 of these Arrangements
- 4.11. The Data Protection Leads must comply with these Arrangements.

### **Lead for Data Subject Rights**

4.12. The Lead for Data Subject Rights acts as the contact point for Data Subjects as required by [Section 58\(3\) of the DPA](#) for Law Enforcement Purposes. Under [Article 26\(3\) of the UK GDPR](#) Data Subjects may exercise their rights to any of the Joint Controllers, but are encouraged to do so via the Lead for Data Subject Rights. Also see sections 10 & 11 of these Arrangements.

4.13. The Lead for Data Subject Rights must comply with these Arrangements.

#### **NPCC Data Protection Officer (DPO)**

4.14. The NPCC DPO must undertake, as a minimum, the tasks set out under [Section 71 of the DPA](#) and [Article 39 of the UK GDPR](#) in respect of processing of Personal Data under the scope of these Arrangements.

4.15. In support of the DPO's statutory task to monitor compliance with the DPA and UK GDPR they will monitor compliance with these Arrangements.

## **5. Damages - liability**

5.1. Clause 19 of the NPCC 22A is modified as follows: any liabilities incurred in relation to the data controllership, FOIA and EIR arrangements set out in this Agreement shall be dealt with in accordance with Clause 19 of the NPCC 22A save that:

- Each Joint Controller is individually responsible for any damage caused by the processing of Personal Data by its organisation, which is found to be in breach of the DPA or UK GDPR
- In the event of a dispute between the Joint Controllers in respect of the responsibility for the damage caused by the Joint Processing carried out by one of more of the Joint Controllers in accordance with these Arrangements, the Joint Controller responsible for settling the penalty imposed is as determined by the ICO in the exercise of their enforcement powers under the DPA

## **6. Data Subject Rights**

6.1. The Lead for Data Subject Rights acts as the primary point of contact for Data Subjects wishing to exercise their rights under [Part 3 of the DPA](#) and/or [Chapter III of the UK GDPR](#).

6.2. The Lead for Data Subject Rights has established the procedure to be followed by the Joint Controllers in respect of the management of Data Subject Rights applications relating to any Joint Processing carried out under these Arrangements.

6.3. The Joint Controllers will individually provide such assistance as is reasonably required to enable the Lead for Data Subjects to comply with applications from Data Subjects exercising their rights under the DPA within time limits imposed by the legislation.

6.4. In respect of Personal Data subject to Joint Processing the relevant Joint Controllers will individually notify the Lead for Data Subjects within 24 hours or, where that is not possible, as soon as reasonably practicable after becoming aware if they:

- receive a Right of Access application
- receive an application for rectification of Personal Data
- receive an application for erasure or restriction on processing of Personal Data
- receive any other application, request, complaint or communication relating to any of the Joint Controllers' obligations under Part 3 of the DPA

## **7. Freedom of Information (FOI) and Environmental Information Regulations (EIR) Applications<sup>2</sup>**

- 7.1. The Lead for Data Subject Rights acts as the primary point of contact for 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 relating information held under these Arrangements by those Joint Controllers who are subject to FOI and EIR.
- 7.2. The Lead for Data Subject Rights has established the procedure to be followed by the Joint Controllers in respect of the management of FOI and EIR applications.
- 7.3. All Joint Controllers will maintain a point of contact (SPoC) with whom the Lead for Data Subjects will liaise as necessary for the management of FOI and EIR applications.
- 7.4. The Joint Controllers will individually provide such assistance as is reasonably required to enable the Lead for Data Subjects to respond to FOI and EIR applications from individuals within time limits imposed by the legislation.
- 7.5. In respect of FOI and EIR applications the relevant Joint Controllers will individually notify the Lead for Data Subjects within 24 hours or, where that is not possible, as soon as reasonably practicable after becoming aware if they:
  - receive a FOI or EIR application
  - receive any other request, complaint or communication relating to any of the Joint Controllers' obligations under FOI or EIR
- 7.6. The Lead for Data Subject Rights is responsible for ensuring that a Publication Scheme is maintained in accordance with FOI.

## **8. Data retention and deletion**

- 8.1. Each Joint Controller will only retain or process Personal Data for as long as is necessary in connection with the purposes it is retained in accordance with legislation and relevant national or local guidelines.

## **9. Security and Training**

- 9.1. 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.
- 9.2. 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.
- 9.3. 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.

---

<sup>2</sup> The DPA and UK GDPR do not place a requirement for FOI and EIR arrangements to be included in Joint Controller Arrangements, but these are included for completeness.

## **10. Personal Data Breaches and reporting procedures**

- 10.1. Each Joint Controller is responsible for reporting any actual or suspected Personal Data Breach relating to Personal Data processed under these Arrangements for NPCC functions identified by its staff to the NPCC DPO. The NPCC DPO will be responsible for deciding whether the 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.
- 10.2. The Joint Controller should report any actual or suspected Personal Data Breach to the NPCC DPO without undue delay.
- 10.3. In the event that a Joint Controller becomes aware of any Data Protection Breach committed by the staff of another Joint Controller they will inform that Joint Controller's DPO and the NPCC DPO without undue delay.
- 10.4. The relevant Joint Controllers will provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

## **11. Data Sharing**

- 11.1. In recognition of a long-established existing convention, the NPCC Controllers, whether acting as Joint Controllers or as independent Controllers confirm that there is no compulsion arising from these Arrangements for Data Sharing Agreements to be created to cover the sharing of Personal Data between them either within the context of these Arrangements or beyond them.

## **12. Data Governance of National Datasets**

- 12.1. The NPCC Controllers recognise that they and other Controllers have Data Protection obligations with regards to the Personal Data processed by them within National Datasets.
- 12.2. In 2023 the definition of 'National Dataset' was agreed by the NPCC Digital, Data and Technology (DDaT) Co-ordination Committee as follows:
  - A 'Dataset' is an organised collection of data held digitally
  - A 'National Dataset' is a dataset containing Personal Data that is readily accessible by more than one NPCC police force and is either:
    - Processed in IT infrastructure implemented by the Home Office Police and Public Protection Technology (PPPT) portfolio or the Police Digital Service (PDS) (or their predecessors/successors), or
    - Designated as such by the dataset's police force Joint Controllers, or
    - Designated as such by the National Policing Data & Analytics Board
- 12.3. The DDaT Co-ordination Committee also agreed on an initial list of National Datasets, a process for formally accepting additional ones and the NPCC Data Governance Framework for National Datasets to be implemented for each of them.
- 12.4. The NPCC Controllers confirm that:
  - the Chair of DDaT Co-ordination Committee is authorised to designate Lead Controllers or Data Protection Leads for National Datasets

- the designated leads of National Datasets will enter into Joint Controllership Agreements for the Personal Data processed in their respective National Datasets
- under such Joint Controllership Agreements, the Lead Controllers or Data Protection Leads must ensure that compliance activities occur equivalent to those set out under clauses 4.4 & 4.5 of these Arrangements
- under such Joint Controllership Agreements, the Lead Controllers or Data Protection Leads are authorised to undertake activities equivalent to those set out under clause 4.6 of these Arrangements
- the Lead Controllers or Data Protection Leads for National Datasets must meet the requirements of the NPCC Data Governance Framework for National Datasets
- they acknowledge that some National Datasets will have Joint Controllers beyond the NPCC Joint Controllers
- they acknowledge the existing convention that the Chair of DDaT Co-ordination Committee acts as the National SIRO for National Datasets

### **13. Data Protection Governance of National Units outside scope of these Arrangements**

13.1. The NPCC recognises that some National Units have been established with their own Data Protection Governance arrangements distinct from these Arrangements. These Arrangements are not intended to interfere with those already established for certain National Units.

### **14. Use of Agents to enter into Data Processing Contracts**

- 14.1. The NPCC recognises that circumstances arise where the NPCC Chief Officers each independently appoint the same Processor to process Personal Data in a consistent way, beyond of the scope of their Joint Controllership.
- 14.2. In such circumstances the Joint Controllers authorise the relevant Lead Controller, or (where authority has been delegated under Clause 3.5 above) Data Protection Lead, to act as Agent for the Joint Controllers by negotiating, executing and concluding Data Processing Contracts with the Processor or Processors for and on behalf of the Joint Controllers.
- 14.3. This obviates the need for each NPCC Chief Officer to enter into one of multiple Data Processing Contracts with the Processor.
- 14.4. The Joint Controllers may designate an Agent who is not a Lead Controller or Data Protection Lead if written consent is obtained from the NPCC Chief Officers concerned. The NPCC has developed templated letters, forms and a process to assist this activity.<sup>3</sup>

---

<sup>3</sup> In 2023 this process was used to create a single Data Processing Contract between the NPCC Chief Officers and the Home Office for the National Data Quality Improvement Service (NDQIS), and to empower the Chief Officer leading the Performance Co-ordination Committee to enter into future Data Processing Contracts on their behalf as the need arose.

## **15. Review and governance of these Arrangements**

- 15.1. These Arrangements will remain in force until terminated by a majority number of the Joint Controllers and following a review as at clause 15.2.
- 15.2. The Chair of the DDaT Co-ordination Committee 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, a review an immediate review of these Arrangements. The Joint Controllers may decide to continue, amend or terminate these Arrangements depending on the outcome of any review.
- 15.3. The review set out at clause 15.2 will involve:
  - Assessing whether the purposes of Joint 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 (policy) is being complied with
  - Assessing whether Personal Data Breaches involving data have been handled in accordance with these Arrangements and the relevant legal framework
- 15.4. The Joint Controllers will provide reasonable assistance as is necessary to facilitate the conduct of any review in an efficient and expeditious manner.

## **16. Approval and Adoption**

- 16.1. These Arrangements were approved and adopted by the Chair of the NPCC Digital, Data and Technology Co-ordination Committee on behalf of the Joint Controllers on 7<sup>th</sup> June 2024.

## **Schedule 1 - Police Joint Controllers**

The Chief Officers of the Police Forces listed below are Joint Controllers under these Arrangements. Each Chief Officer is a Party to the NPCC 22A.

Avon & Somerset Constabulary  
Bedfordshire Police  
British Transport Police  
Cambridgeshire Constabulary  
Cheshire Constabulary  
City of London Police  
Civil Nuclear Constabulary  
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  
Ministry of Defence Police  
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 – NPCC JCA Summary of Roles, Designations and Responsibilities

<b>Roles</b>	<b>Designations</b>	<b>Responsibilities</b>
Joint Controllers	46 Chief Officers listed in Schedule 1	Data Protection compliance for NPCC
Lead Controllers	Chief Officers who chair Co-ordination Committees Chief Officers who lead National Units Chief Officers who lead NPCC Programmes	Ensuing specified Data Protection compliance activities occur in their entities and sub-structures.  Authorised to enter into National DSAs, MOUs, JCAs, appoint Processors, in compliance with Schedule 2  Can delegate those specified activities and authorisations to Data Protection Leads
Data Protection Leads	Leads of NPCC Portfolios, Sub-Committees, Working Groups, & other sub-structures	Specified Data Protection compliance activities & authorised activities as delegated by Lead Controllers
	National Unit leads & NPCC Programme leads who are not Chief Officers	Specified Data Protection compliance activities & authorised activities within their entities and sub-structures
	NPCC Chair	Specified Data Protection compliance activities & authorised activities for admin of CCC & Strategic Hub only
Lead for Subject Rights	National Police Freedom of Information and Data Protection Unit (NPFDU).	Management of rights applications under Data Protection legislation  Management of FOI and EIR requests for information
NPCC DPO	NPCC DPO	As a minimum tasks set out under <a href="#">Section 71 of the DPA</a> and <a href="#">Article 39 of the UK GDPR</a> including monitoring compliance with these Arrangements

<b>Roles</b>	<b>Designations</b>	<b>Responsibilities</b>
NPCC SIRO	Chair of NPCC	As per <a href="#">SIRO Handbook</a> (excludes National Databases for which the DDaT CC Chair is National SIRO)
IAOs	Chairs Co-ordination Committees National Unit leads NPCC Programme leads	As per <a href="#">IAO Handbook</a> in their entities and sub-structures.
	NPCC Strategic Hub Lead	As per <a href="#">IAO Handbook</a> for admin of CCC & Strategic Hub only

**Schedule 3 – Arrangements for the quality assurance and approval of National Agreements related data sharing under the NPCC**



**NPCC DATA SHARING QUALITY ASSURANCE PROC**



