# Information Sharing Agreement

## Between

## National Police Chiefs' Council
## ACRO Criminal Records Office

## And

## The Information Commissioner

## Summary Sheet

| Freedom of Information Act Publication Scheme | |
|---|---|
| **Security Classification (GSC)** | OFFICIAL |
| **Publication Scheme Y/N** | Yes |
| **Title** | Information Sharing Agreement between ACRO Criminal Records Office (ACRO) and the Information Commissioners (IC). |
| **Version** | 2.0 |
| **Summary** | This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for the ACRO, acting on behalf of UK police forces that are subject to the ACRO section 22A Collaboration Agreement, to provide ICO with access to relevant information held on the Police National Computer (PNC), in support of the IC's regulatory and enforcement powers under the Data Protection Legislation .This includes provision of convictions, cautions, reprimands and final warnings for the investigation and prosecution of offences under the Data Protection Act 2018 (DPA) and Freedom of Information Act 2000 (FOIA), and in the limited circumstances of civil enforcement under the United Kingdom General Data Protection Regulation (UK GDPR) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011 (PECR). The nature of the information needed by the ICO includes both recordable and non-recordable offences.<br><br>Furthermore, this Agreement also allows for the recording of the details of individuals, prosecuted by the IC under the Data Protection Legislation, as required by the National Police Records (Recordable Offences Regulations 2000 (SI 2000/1139), onto PNC, on behalf of the IC. |
| **Author** | ****, ACRO Information Governance Officer |
| **Date Issued** | 10/07/2024 |
| **Review date** | 10/04/2025 |
| **Expiry date** | 10/07/2025 |
| **ISA Reference** | ACRO/042 |
| **Location of Agreement** | ACRO ISA Library |
| **ACRO DPIA Reference** | DPIA 042 |

## Contents

# Version control

| Version No. | Date | Amendments Made | Authorisation |
|---|---|---|---|
| 0.1 – 1.0 | 20/07/2020 | Renewal transfer to updated template, drafting and 2022/23 Renewal finalised | ACRO and ICO |
| 1.1 | 08/09/2023 | 2023/24 Annual renewal draft | MH, ACRO |
| 1.2 | 08/01/2024 | DPO Review | AAS, ACRO |
| 1.3 | 15/01/2024 | ICO Review | ICO |
| 1.4 | 01/03/2024 | DPO Review | AAS, ACRO |
| 1.5 | 20/03/2024 | ICO review | ICO |
| 1.6 | 18/04/2024 | ACRO SIRO Sign off | JF, ACRO |
| 1.7 | 10/06/2024 | Correction to ASN Creation service | MH, ACRO |
| 2.0 | 10/07/2024 | NPCC Final Sign off | NPCC |

# 1. Parties to the Agreement

1.1. ACRO Criminal Records Office
PO Box 481
Fareham
PO14 9FS

1.2. The Information Commissioner (The IC)
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

# 2. Agreed Terms

2.1. **Interpretation**

The following definitions and rules of interpretation apply in this Agreement.

2.1.1. Definitions:

**ACRO:** ACRO Criminal Records Office.

**Agreed Purpose**: has the meaning given to it in clause 3.2 of this Agreement.

**ASN**: Arrest Summons Number.

**Business Day**: a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

**Business Hours**: 9:00 am to 5:00 pm Monday to Friday on a day that is not a public holiday.

**CEO:** Chief Executive Officer.

**CPS:** Crown Prosecution Service.

**Criminal Offence Data** is personal data relating to criminal convictions and offences or related security measures and includes personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. (DPA 2018, section 11(2)).

**Data Protection Legislation**: all applicable data protection and privacy legislation, regulations and guidance including Regulation (EU) 2016/679, as implemented into UK law by the EU (Withdrawal) Act 2018 and as amended by Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, (**"UK GDPR""**), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**), and any guidance or codes of practice issued by the Supervisory Authority from time to time (all as amended, updated or re-enacted from time to time).

**DCC:** Deputy Chief Constable.

**EIR:** Environmental Information Regulations 2004.

**EU:** European Union.

**FOIA:** Freedom of Information Act 2000. Freedom of Information (FOI).

**GSCP:** Government Security Classification Policy.

**HIOWC:** Hampshire & Isle of Wight Constabulary.

**IC:** Information Commissioner- and any reference to the Commissioner or the IC shall include his statutory successors.

**ICO:** Information Commissioner's Office

**MB:** Megabyte (of data).

**NFA:** No Further Action.

**NPA:** Non-Police Agency.

**NPCC:** National Police Chiefs' Council.

**NPPA:** Non-Police Prosecuting Agency.

**OCiP:** Operational Communications in Policing.

**OIC:** Officer in charge of the case.

**Offences:** a breach of a law or rule; an illegal act.

**PECR :** The Privacy and Electronic Communications (EC Directive) Regulations 2003

**Personal Data** shall have the meaning given to it in the Data Protection Legislation. Personal Data is defined as any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (UK GDPR, Article 4).

**Personal Data Breach** shall have the meaning given to it in the Data Protection Legislation.

**PNC:** Police National Computer.

**Section 22A Agreement:** An agreement made pursuant to section 22A of the Police Act 1996 (as amended) enables police forces, local policing bodies as defined in that Act and other parties as defined in that Act to make an agreement about the discharge of functions by officers and staff, where it is in the interests of the efficiency or effectiveness of their own and other police force areas. By entering into this Agreement, the Parties have taken account of the statutory guidance for police collaboration published by the Home Office in October 2012 in exercise of the Home Secretary's power under section 23F of the Police Act 1996, to provide guidance about collaboration agreements and related matters.

**Shared Personal Data**: the personal data to be shared between the parties under clauses 5.1.2 and 5.2.2 of this Agreement.

**SIRO:** Senior Information Risk Owner.

**SPOC:** Single Point of Contact.

**Subject Information Rights**: means the exercise by a data subject of his or her rights under Articles 13 to 22 of the UK GDPR or sections 45 to 49 of the DPA 2018.

**Supervisory Authority:** the Information Commissioner or country equivalent.

**UK:** United Kingdom.

**WinZip:** trialware file archiver and compressor for Microsoft Windows.

**WM:** Wanted Missing report.

2.1.2. **Controller**, **Processor**, **Data Subject** and **Personal Data**, **Special Categories of Personal Data**, **Processing, Sensitive Processing** and "**appropriate technical and organisational measures**" shall have the meanings given to them in the Data Protection Legislation.

2.1.3. Clause and paragraph headings shall not affect the interpretation of this Agreement.

2.1.4. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

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

2.1.6. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

2.1.7. A reference to **writing** or **written** includes e-mail.

2.1.8. Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.

# 3. Purpose and background of the Agreement

## 3.1. Background

3.1.1. ACRO is a national police unit, under the National Police Chiefs' Council (NPCC) working for safer communities. ACRO is the national police unit responsible for exchanging criminal conviction information between the United Kingdom (UK) and other countries. ACRO provides access to information held on PNC to support the criminal justice work of some Non-Police Prosecuting Agencies (NPPAs) and assists safeguarding processes conducted by relevant agencies.

3.1.2. The Commissioner (IC) is a corporation sole appointed by His Majesty the King under the Data Protection Acts 1984, 1998 and 2018, to act as the UK's independent regulator – promoting public access to official information and protecting personal information.

3.1.3. The IC is a Competent Authority and Regulatory Body for both Part 2 and 3 processing under the Data Protection Act 2018. Article 57 of the UK GDPR and section 115(2)(a) of the DPA place a broad range of statutory duties on the IC, including monitoring and enforcement (both criminal and civil) of the UK GDPR, promotion of good practice and adherence to the data protection obligations by those who process data. The IC also has duties under the Investigatory Powers Act 2016 and Freedom of Information Act 2000.

## 3.2. Purpose

3.2.1. This Agreement sets out the framework for the sharing of Personal Data between ACRO (acting as Processor on behalf of the Chief Constables as Controller, and as further described in clause 4.4), and the IC. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

3.2.2. The purpose of this Agreement is to formalise the arrangements for ACRO, acting on behalf of UK police forces that are subject to the ACRO section 22A Collaboration Agreement, to provide the ICO with access to relevant information held on PNC, specifically convictions, cautions, reprimands and final warnings. It is necessary for the IC to have access to such information for the investigation and taking of civil enforcement action, and the investigation and prosecution of criminal and civil offences under the Data Protection Legislation (including PECR) and the Freedom of Information Act 2000. It is also necessary for the ICO to have access to such information in other limited, specific circumstances, particularly in order to conduct a risk assessment prior to exercising a warrant in connection with potential civil enforcement action under section 149(2) of the Data Protection Act 2018 or in connection with the IC's powers under PECR. The nature of the information needed by the ICO includes both recordable and non-recordable offences.

3.2.3. Under this Agreement, the IC can request that ACRO create records on PNC for the purpose of prosecuting individuals under the Data Protection Act 2018 in respect of the recordable offences set out in section 199 of the DPA, as provided for in The National Police records (Recordable Offences) Regulations 2000, and other recordable offences where the ICO act as the prosecuting agent. These will be updated on to the PNC.

3.2.4. The aim of the data sharing initiative is to provide PNC data required by the IC for recordable and non-recordable offences. It will serve to benefit society by investigating and prosecuting offences where the safety and security of personal data has been jeopardised.

3.2.5. This Agreement will be used to assist in ensuring that:

a) Personal Data is shared in a secure, confidential manner with designated points of contact;
b) Personal Data is shared only on a 'need to know' basis;
c) Shared Personal Data will not be irrelevant or excessive with regards to the Agreed Purpose (i.e. the Civil Enforcement Purpose or Criminal Enforcement Purpose, as applicable and as further defined below);
d) There are clear procedures to be followed with regard to Shared Personal Data;
e) Personal Data will only be used for the reason(s) it has been obtained;
f) Data quality is maintained and errors are rectified without undue delay;
g) Lawful and necessary re-use of Personal Data is done in accordance with Data Protection Legislation; and
h) Subject information rights are observed without undue prejudice to the lawful purpose of either party.

3.2.6. The parties agree to only process Shared Personal Data, (i) in the case of the IC to discharge their statutory functions, primarily in relation to criminal enforcement but also in very limited and specific scenarios prior to civil enforcement; and (ii) in the case of ACRO, for maintenance of centralised records on the PNC. The parties shall not process Shared Personal Data in a way that is incompatible with the Civil Enforcement Purposes and/or Criminal Enforcement Purposes, as applicable and as defined in clause 5 below. ("**Agreed Purpose**").

# 4. Powers

## 4.1. ICO Legal Basis

4.1.1. For the purposes of this part, "the law enforcement purposes" are as set out in the Data Protection Legislation.

4.1.2. The ICO is a Competent Authority under Schedule 7 of the Data Protection Act (DPA) 2018.

## 4.2. Civil Enforcement

4.2.1. The ICO is empowered under section 154 and Schedule 15 of the Data Protection Act 2018 to seek a warrant imbuing it with the power of entry and inspection in respect of civil investigations relating to potential infringements of section 149(2) of the Data Protection Act 2018. Under Regulation 31(1) of PECR, certain provisions of the Data Protection Act 1998 (the DPA 1998) relating to the IC's enforcement functions remain in force for the purposes of PECR. The provisions of Part V of the DPA 1998 and of Schedules 6 and 9 of the DPA 1998 are extended for the purposes of PECR, subject to the modifications set out in Schedule 1 of PECR including Part V and sections 55A to 55E (dealing with monetary penalties), Schedule 6 (Appeal proceedings), and Schedule 9 (Powers of entry and inspection) of the DPA 1998. Paragraph 58, Schedule 20 of the DPA 2018 provides that the repeal of provisions of the DPA 1998 does not affect its operation for the purposes of PECR.

4.2.2. The ICO may require, upon request, access to Shared Personal Data in connection with the purpose outlined in clause 4.3.1 in order to carry out a risk assessment prior to exercising a warrant or in connection with PECR enforcement as outlined in 4.2.1 (**"the Civil Enforcement Purposes"**).

4.2.3. Processing of Shared Personal Data for Civil Enforcement Purposes is lawful on the basis that, in accordance with Article 6(1):

(e), it is necessary in the exercise of official authority.

4.2.4. Insofar as the Processing of Shared Personal Data for Civil Enforcement Purposes also entails Processing of Special Categories of Personal Data then that is lawful on the basis that, in accordance with Article 9(2):

(g), it is necessary for reasons of substantial public interest.

4.2.5. It satisfies a condition in Schedule 1, Paragraph 6 of the Data Protection Act 2018 in relation to a function conferred by an enactment or rule of law.

4.3. **Criminal Enforcement**

4.3.1. The ICO is also responsible for investigating and prosecuting the following offences:

- Data Protection Act 2018, section 119: Intentionally obstructing, or failing to assist the IC in inspecting personal data where the inspection is necessary in order to discharge an international obligation (subject to restrictions).
- Data Protection Act 2018, section 132: A current or previous member of the IC's Staff or an agent of the IC disclosing information obtained, or provided to, the IC in the course of, or for the purposes of, the discharging of his functions without lawful authority.
- Data Protection Act 2018, section 144: Making a false statement in response to an information notice.
- Data Protection Act 2018, section 148: Destroying or falsifying information and documents etc.
- Data Protection Act 2018, section 170: Unlawful obtaining of personal data.
- Data Protection Act 2018, section 171: To knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.
- Data Protection Act 2018, section 173: To alter, deface, block, erase, destroy or conceal information with the intention of preventing access to information to which a data subject would be entitled to under a data subject right.
- Data Protection Act 2018, section 184: To require another person to provide a relevant record in connection with the recruitment or continued employment of that person (enforced subject access).
- Data Protection Act 2018, Schedule 15, para.15: To intentionally obstruct a person in the execution of a warrant issued under the DPA, to fail to provide assistance in the execution of such a warrant or to make a false statement.
  And,

- Freedom of Information Act 2000, section 77: the offence of altering, defacing, blocking, erasing, destroying or concealing any record, with the intention of preventing the disclosure of information to which an applicant would have been entitled.

4.3.2. The ICO may require, upon request, the Shared Personal Data in order to investigate and prosecute the offences outlined in clause 4.3.1 (**"the Criminal Enforcement Purposes"**).

4.3.3. Processing of personal data for any of the Criminal Enforcement Purposes is lawful where that processing is necessary for the performance of a task carried out for that purpose by a Competent Authority, (s.35(2)(b)).

4.3.4. Sensitive processing of Personal Data is lawful for Criminal Enforcement Purposes where it is processed in accordance with section 35(5) of the Data Protection Act 2018 and meets a condition in Schedule 8. Processing under this Agreement meets conditions (1) Statutory etc. purposes and (2) Administration of Justice.

4.4. **ACRO Legal Basis**

4.4.1. Section 22A of the Police Act 1996 enables police forces to discharge functions of officers and staff where it is in the interests of efficiency or effectiveness of their own and other police force areas. Schedule 7, Paragraph 17 of the DPA 2018 establishes bodies created under section 22A of the Police Act 1996 as Competent Authorities.

4.4.2. ACRO, hosted by Hampshire & Isle of Wight Constabulary (HIOWC), is established as a Data Processor, through the National Police Collaboration Agreement relating to ACRO under section 22A of the Police Act 1996. This Agreement gives ACRO the authority to act on behalf of the Chief Constables, the Joint Data Controllers, to provide PNC enquiry, update and disclosure services to Non-Police Agencies (NPAs) and NPPAs.

4.4.3. ACRO is a Competent Authority, by virtue of the section 22A Agreement, processing data for a law enforcement purpose. ACRO specifically confirms and agrees that by entering into this agreement it has the necessary legal authority to do so, and in particular that the section 22A Agreement legitimately establishes ACRO as a Data Processor acting under the instructions of the Chief Constables as individual Data Controllers for the information held on PNC and that the section 22A Agreement enables ACRO to lawfully share personal data with the ICO for a Civil Enforcement Purpose or Criminal Enforcement Purpose. All references to ACRO throughout this agreement should be read and interpreted in accordance with this clause 4.4.

4.4.4. Under the first Data Protection Principle, processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law. Under section 35(2) of the DPA 2018 the following applies:

- The processing is necessary for the performance of a task.

4.4.5. Under section 35 (3) to (5) and Schedule 8 of the DPA 2018, ACRO meets the conditions for sensitive processing as follows:

- Administration of justice;

4.5. **Code of Practice for the Management of Police Information**

4.5.1. This Agreement outlines the need for the Police and Partners to work together to share information in line with the Policing Purposes as set out in

the Management of Police Information Code of Practice. In line with section 39A of the Police Act 1996, Chief Officers are required to give "due regard" to this statutory code. The Policing Purposes summarise the statutory and common law duties of the police service for which personal data may be processed and are described as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice; and
- Any duty or responsibility arising from common or statute law.

4.6. **Human Rights Act 1998**

4.6.1. Under Schedule 1, Article 8 of the Human Rights Act 1998, all data subjects have a right to respect for their private and family life, home and correspondence.

4.6.2. Interference with this right may be justified when lawful and necessary and in the interests of:

- Discharging the common law police duties;
- Preventing/detecting unlawful acts;
- Protecting the public against dishonesty, etc.;
- Preventing fraud;
- Terrorist finance/money laundering;
- Safeguarding children and adults at risk;
- Safeguarding the economic wellbeing of vulnerable adults.

4.7. **Common Law Police Disclosure**

4.7.1. Where legislation provides the organisation with a power to process Personal Data for a specific purpose, but there is no explicit legislative authority, Common Law Police Disclosure ensures that where there is a public protection risk, the police will pass information to the employer or regulatory body to allow them to act swiftly to mitigate any danger. This only applies where there is a pressing social need.

4.8. **Crime and Disorder Act 1998**

4.6.1 Under section 17 the Relevant Authority has the duty to consider crime and disorder implications and the need to do all that it reasonably can to prevent:

- Crime and disorder in its area (including anti-social and other behaviour adversely affecting the local environment); and
- The misuse of drugs, alcohol and other substances in its area; and
- Re-offending in its area.

4.6.2 Under section 115(1) any person who would not have power to disclose information to a Relevant Authority or to a person acting on behalf of such

an Authority shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.

4.9. **The Policing Protocol Order 2011**

4.7.1 The Chief Constable is responsible for maintaining the King's Peace and is accountable in law for the exercising of police powers and to the Police and Crime Commissioner (PCC) for delivering efficient and effective policing, management of resourcing and expenditure by the police force.

# 5. Process

5.1. **Overview**

5.1.1. ACRO, in response to requests made by the IC, will create an Arrest Summons Number (ASN) on the PNC in relation to the impending prosecution, will conduct PNC searches and provide a PNC print to meet their information needs.

5.1.2. The PNC data will comprise of:

a) A Disclosure PNC print. The personal data disclosed under this print includes (if available): name, date of birth, birth place, sex, address, occupation, aliases (including Driver and Vehicle Licensing Agency (DVLA) name) and alias dates of birth. The home address that is printed in the ID part of the print is decided by the following rules:
   - If there is more than one home address on the record, the most recent address is used;
   - If there is no home address present, the most recent 'no fixed abode' address type will be used;
   - If neither of the above address types are present, the most recent 'Other' address is printed.

b) A Prosecutor's and Court Multiple print. The personal data disclosed under this print includes (if available): name, date of birth, birth place, address, driver number, aliases (including DVLA name) and alias dates of birth. The home address that is printed in the ID part of the print is decided by the following rules:
   - If there is more than one home address on the record, the most recent address is used;
   - If there is no home address present, the most recent 'no fixed abode' address type will be used;
   - If neither of the above address types are present, the most recent 'Other' address is printed.

5.1.3. If relevant, ACRO shall provide to the IC, for onward provision to the court, a PNC Prosecutor's and Court Multiple Print showing the subject's previous convictions, warnings and reprimands, if any exist. This information shall only be provided as part of the ASN creation process in relation to a current prosecution.

5.1.4. The IC Officer will review all referred information and may ask for additional information to aid decision making.

5.1.5. Where an offence has been committed resulting in a conviction in court or a caution, reprimand or warning, ACRO will record this information on the PNC as required by The National Police Records (Recordable Offences) Regulations 2000 (SI 2000/1139), on behalf of the IC.

5.2. **PNC Searches**

5.2.1. Requests for a PNC search are to be made by the IC on a 'Names Enquiry' spreadsheet which will be supplied by ACRO separately.

5.2.2. The following Personal Data is to be provided in support of each request (where known):

- First name;
- Any middle names;
- Surname/family name;
- Date of birth (dd/mm/yyyy);
- Any alias details (names, dates of birth etc.);
- Place of birth (where known);
- Address;
- ICO case reference.

5.2.3. In the event that no convictions are found on the PNC or the subject of the enquiry is 'No Trace', a response stating 'no relevant information held on PNC in relation to the subject of your enquiry' will be sent to the IC. In the absence of fingerprints the identity of the subject cannot be verified. Similar wording will apply to 'Trace' returns i.e. when a record is found and a PNC print provided.

5.3. **Additional Information Requirements**

5.3.1. Other personal data, which the ICO Officer may be aware of e.g. National Insurance Number, Passport or Driving Licence Number etc. can be provided to aid identification. This additional information will be used to confirm identity and is of particular value where the name or other personal details are identical on the PNC.

5.3.2. It is not necessary to obtain the additional information as a matter of course particularly if it is not currently recorded as part of the IC normal administrative procedures.

5.3.3. If required, ACRO will seek additional information from the IC to verify the identity of the subject of the request via the following ICO mailboxes:

****@ico.org.uk
****@ico.org.uk
****@ico.org.uk
****@ico.org.uk

5.3.4. All e-mail communication containing personal and conviction data shall be protected in compliance with the Government's Minimum Cyber Security Standard (GMCSS).

5.3.5. No other mailboxes are to be used unless this Agreement is updated to reflect a change of 'nominated' point of contact for the IC.

5.3.6. Where appropriate, the IC will make contact with the subject of the enquiry to seek the additional information required by ACRO.

**5.4 Contingency Backup**

5.4.1 In an event where the ICO require ACRO to provide a contingency service for PNC requirements in line with the Agreed Services, discussion must be had, prior to any checks, in order to establish volumes and expected turnaround times. This is necessary in order to ensure ACRO can provide the required service and cope with the demand.

# 6. Submission

## 6.1. Names Enquiry Spreadsheets

6.1.1. Completed 'Names Enquiry' spreadsheets are to be sent via secure e-mail to the following e-mail address: ****@acro.police.uk

6.1.2. ACRO will receive requests from the IC, via the following secure mailbox:
****@ico.org.uk
****@ico.org.uk
****@ico.org.uk
****@ico.org.uk

6.1.3. Erroneous or incomplete 'Names Enquiry' spreadsheets will not be processed. They will be returned to the IC as invalid and a reason provided.

## 6.2. Telephone Requests

6.2.1. Requests may be made by telephone in cases of emergency. A 'Names Enquiry' spreadsheet must be submitted in advance, and a call to expedite an existing check may then be made. This ensures ACRO have all the necessary details for accurate data processing.

6.2.2. Such requests can only be made by a limited number of the Agency's staff. As at the date of this Agreement, the ICO staff who will have the ability to make telephone requests shall be:

- **** (Head of Intelligence);
- **** (Group Manager, High Priority Investigations and Intelligence);
- **** (Group Manager, Intelligence); and
- **** (Team Manager, High Priority Investigations and Intelligence).

6.2.3. The ICO may update this list by notice to ACRO from time to time.

# 7. Provision of Information

7.1. **Response to a PNC Names Enquiry Search**

7.1.1. In response to a formal written or verbal (including telephone) application, ACRO will provide a Disclosure Print to the IC with the following information derived from PNC in response to applications made in accordance with this Agreement:

- All convictions, cautions, warnings and reprimands.
- Additional information as deemed relevant by ACRO where there is a pressing social need to do so (via a Force Disclosure Unit as appropriate).

7.1.2. It should be noted that the service provided under this Agreement only covers the provision of certain PNC prints depending on the request submitted by the ICO.

7.1.3. If the IC requires an additional copy of the 'Prosecutor's and Court Multiple Print' then this should be made clear in the correspondence submitted by the IC. Such requests will be charged in accordance with the letter of charges provided separately to the IC.

7.1.4. PNC Warning Signals are not disclosed on Disclosure or Court Multi-prints. However, if the IC wishes to confirm whether a Warning Signal is recorded on PNC for an individual under investigation, confirmation can be sought through ACRO.

7.1.5. Such requests will be completed on an ad hoc basis and will only be subject to disclosure on the basis that the IC explicitly requests this. However, it should be noted that Warning Signals are not held on PNC records. It is therefore of high possibility that a nil to low return will be provided for any requests submitted by the IC.

7.1.6. The types of Warning Signals that will be disclosed will be limited to only those relating to violence, conceals, weapons or firearms, where a risk could be posed to ICO Officers who require attendance at the subject's abode. ACRO will then determine whether the disclosure of such Warning Signals is warranted based on the information provided by the IC.

7.1.7. It should be noted that the service provided under this Agreement only covers the provision of certain PNC prints depending on the request submitted by the IC.

7.1.8. If the IC has a secondary query or wishes to follow-up on the PNC information provided, a formal request is to be made through the nominated ACRO mailbox: ****@acro.police.uk

7.1.9. The IC will need to liaise directly with forces to obtain further explanation of specific information regarding the offending revealed in the prints provided under this Agreement or to gain access to statements, interviews under caution etc. relating to any previous offending. Forces may apply their own charges in respect of any information they disclose.

# 8. Recording Convictions on the PNC

## 8.1. Creating Records on the PNC

8.1.1. The process for creating records and assigning Arrest Summons Numbers (ASN) to prosecutions brought by Non-Police Prosecuting Agencies (NPPA) is contained in the 'National Standard for Recording NPPA Prosecutions on the Police National Computer' (the '**National Standard**').

8.1.2. The IC undertakes to adhere to the requirements of the National Standard including the requirement to complete and submit the required NPPA form in the agreed format together with a copy of the relevant information to the court in order for a record to be created on the PNC. Court dates are to be provided if known at the time of submission.

8.1.3. The IC will supply a duly completed NPPA form in respect of every person for whom a PNC record is to be created. An ASN will be provided by ACRO in return. A delay in the process is likely to occur if the information provided on the NPPA form by the ICO is incomplete or inaccurate.

8.1.4. As part of the record creation service provided by ACRO, the ICO will be sent a PNC Prosecutor's and Court Multiple print for each ASN created. The multi-prints consists of a Prosecutor's Print plus a Court/Defence/Probation Print. The content of each type of print is defined in the list of PNC Printer Transactions, which will be supplied by ACRO separately.

8.1.5. Covering e-mails from ACRO under which the PNC prints will be returned to the ICO will state that in the absence of fingerprints the subject's identity cannot be verified.

8.1.6. When a prosecution by the IC leads to a court appearance, ACRO will update the PNC with the required details of any adjournment or disposal. These details are provided to ACRO through automated processes when the prosecution occurs at a Magistrates' Court. However, these processes do not extend to prosecutions through the Crown Court and therefore the IC is to advise ACRO of any adjournments or disposal handed down by the court using the form, which will be supplied by ACRO separately.

8.1.7. If, once a PNC record has been created by ACRO and an ASN issued to the IC, a decision is taken to deal with the offender by way of an 'Out of Court disposal' or proceedings are otherwise concluded by way of a discontinuance or 'No Further Action' (NFA) disposal, for instance on the advice of the Crown Prosecution Service (CPS), the IC will inform ACRO as soon as reasonably practical in order that the PNC record can be updated.

# 9. Information Security

## 9.1. Government Security Classification Policy

9.1.1. Parties to this Agreement are to ensure that personal data is handled, stored and processed at OFFICIAL level as defined by the Government Security Classification Policy (GSCP) and may carry the security marking OFFICAL – SENSITIVE, in which case specific handling conditions will be provided. All e-mail communications shall be protected in compliance with the Government's Minimum Cyber Security Standard (GMCSS).

9.1.2. Documents marked using GSCP will describe specific handling conditions to mitigate the risks necessitating such marking. These may include:

a) Any specific limitations on dissemination, circulation or intended audience;
b) Any expectation to consult should re-use be anticipated;
c) Additional secure handling and disposal requirements.

## 9.2. Security Standards

9.2.1. It is expected that parties to this Agreement will have in place baseline security measures compliant with the GMCSS. Parties are at liberty to request copies of each other's:

a) Information Security Policy;
b) Records Management Policy;
c) Data Protection Policy.

9.2.2. Each partner will implement and maintain appropriate technical and organisational measures to:

- Prevent:
  i. unauthorised or unlawful processing of the Personal Data; and
  ii. the accidental loss or destruction of, or damage to, the Shared Personal Data; and
- ensure a level of security appropriate to:
  i. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
  ii. the nature of the Shared Personal Data to be protected.

9.2.3. Any further specific security measures sought by one party shall be notified to the other party from time to time, which shall implement them where reasonably practicable. The parties shall keep such security measures under review and shall carry out updates as they agree are appropriate throughout the Term.

9.2.4. It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures, together with any other applicable data protection laws and guidance, and have

entered into confidentiality agreements relating to the processing of personal data.

9.2.5. Each partner will ensure that employees or agents who have access to personal data have undergone appropriate data protection training to be competent to comply with the terms of this Agreement and Data Protection Legislation.

9.3. **Volumes**

9.3.1. It is estimated that for the year 2024/25, the ICO will request up to 120 PNC Checks and require up to 20 PNC records to be created.

9.3.2. The IC will advise ACRO if the number of PNC Checks and/or PNC Updates is likely to be exceeded.

9.3.3. ACRO will audit requests against the lawful basis and these volumes to ensure that personal data is not being disclosed contrary to the lawful basis and that the agreement is fit to meet any increase in lawful demand.

9.4. **Transmission**

9.4.1. With the exception of telephone requests in cases of emergency, contact between ACRO and the IC should only be made over a secure communication network, via TLS 1.2 e-mail encryption on the part of the IC and an equivalent method on the part of ACRO. Shared Personal Data must be handled with care. Personal data will not be transferred by post.

9.4.2. E-mails must not otherwise be password protected, contain personal data or the descriptor 'Private and Confidential' in the subject field, or be over 6MB in file size.

9.4.3. The ICO reference number must be included in the subject field of every e-mail sent to ACRO.

9.5. **Retention and disposal**

9.5.1. Information shared under this Agreement will be securely stored and disposed of by secure means when no longer required for the purpose for which it is provided as per each parties' Information Security Policy, unless otherwise agreed in a specific case, and legally permitted. Each party will determine and maintain their own retention schedule.

9.5.2. Information held on PNC is governed by the National Retention Schedule. This currently stands at 100 years, or until the subject is deemed to be 100 years of age.

# 10. Information Management

## 10.1. Accuracy of Personal Data

10.1.1. The parties will:

a) comply with Article 5(1)(d) of the GDPR in respect of any Shared Personal Data Processed for Civil Enforcement Purposes; and

b) comply with the fourth data protection principle, as set out in **s**ection 38 of the Data Protection Act 2018, in respect of any Shared Personal Data Processed for Criminal Enforcement Purposes

10.1.2. Where a party rectifies Shared Personal data, it must notify any Competent Authority from which the inaccurate personal data originated, and should notify any other Data Controller of the correction, unless a compelling reason for not doing so exists.

10.1.3. It is the responsibility of all parties to ensure that the information is of sufficient quality for its intended purpose, bearing in mind accuracy, validity, reliability, timeliness, relevance and completeness.

## 10.2. Accuracy Disputes

10.2.1. Should the validity of the information disclosed be disputed by the IC or a third party, the IC will contact ACRO to determine a suitable method to resolve the dispute.

## 10.3. Necessity of Shared Personal Data

10.3.1. The IC and ACRO have, before entering into this Agreement, ensured that the Shared Personal Data to be exchanged between them will comply with:

a) Article 5(1)(c) in respect of Civil Enforcement Purposes; and

b) the third data protection principle, as set out in section 37 of the Data Protection Act 2018, in respect of any Shared Personal Data Processed for Criminal Enforcement Purposes.

## 10.4. Turnaround

10.4.1. This Agreement requires a five *(5)* working day turnaround (not including day of receipt or response) on all requests submitted to ACRO for PNC data, except where ACRO requires further information from the IC to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by the IC.

10.4.2. Responses to requests for additional information must be made by the IC within 10 working days (not including day of receipt or response). If ACRO do not receive the information, the request will be closed.

10.4.3. Information will be exchanged without undue delay. In the event of a delay outside of either party's control, this will be informed to the other party as soon as practical.

10.4.4. An exception to the five *(5)* working day turnaround are those occasions where the conviction data is held on microfiche in the national police microfiche library at Hendon. In these cases, ACRO will provide a response when the required information has been supplied by the custodians of the microfiche.

10.4.5. In some circumstances, the IC may require information urgently, for example, due to ongoing court proceedings. In these circumstances, ACRO will endeavour to complete the check more quickly as agreed with the IC. Such requests will be treated as an exception, and will be considered on a case-by-case basis.

10.4.6. ACRO will complete/update a record on the PNC within 10 working days (not including day of receipt or response) of the receipt of a completed NPA form from the IC in respect of every person for whom a PNC record is to be created.

10.5. **Quality Assurance and Control**

10.5.1. ACRO employ strict quality control procedures and staff undertaking this work are all appropriately trained.

10.5.2. On a monthly basis ACRO can, if required, provide regular management information to the ICO (using the ****@ico.org.uk e-mail address) including:

- Number of PNC 'Names Enquiry' forms received
- Number of PNC Disclosure Prints provided
- Number of Prosecutor & Court Multiprints provided
- Details of any cases that fall outside agreed 'Service Levels'
- Number of issues and/or disputes

# 11. Complaints and Breaches

11.1. **Complaints**

11.1.1. Complaints from data subjects, or their representatives, regarding information held by any of the parties to this Agreement will be investigated first by the organisation receiving the complaint. Each Data Controller will consult with other parties where appropriate.

11.2. **Breaches**

11.2.1. Each party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) Data Subjects under the Data Protection Legislation and shall inform the other party of any Personal Data Breach irrespective of whether there is any requirement to notify any Supervisory Authority or Data Subject(s).

11.2.2. The Parties agree, in particular, to ensure that they comply with:

a) Articles 33 and 34 of the UK GDPR in respect of any Personal Data Breaches affecting Shared Personal Data Processed for Civil Enforcement Purposes; and

b) Sections 67 and 68 of the DPA in respect of any Personal Data Breaches affecting Shared Personal Data Processed for Criminal Enforcement Purposes.

11.2.3. The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

11.2.4. In the event of a dispute or claim brought by a data subject or the Supervisory Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

11.2.5. The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

11.2.6. All security incidents and breaches involving police data shared under this Agreement must be reported immediately to the single points of contact (SPOCs) designated in this document.

# 12. Information Rights

## 12.1. Freedom of Information Act 2000

12.1.1. Where a party to this Agreement is subject to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) all parties shall assist and co-operate with the other to enable the other party to comply with its obligations under FOIA and the EIR. This is in line with the requirements laid out in the Lord Chancellor's Code of Practice issued under section 45 of FOIA.

12.1.2. Where a party receives a request for information in relation to information which it received from the other party, it shall (and will ensure that any sub-contractors it procures shall also):

- Contact the other party within two working days after receipt and in any event within two working days of receiving a request for information;
- The originating authority will provide all necessary assistance as reasonably requested by the party to enable the other party to respond to a request for information within the time for compliance set out in section 10 of the FOIA or Regulation 5 of the EIR.

12.1.3. On receipt of a request made under the provisions of the FOIA in respect of information provided by or relating to the information provided by ACRO, the IC representative is to ascertain whether the NPCC wishes to propose the engagement of any exemptions via the NPCC FOI mailbox: npcc.foi.request@npfdu.police.uk

12.1.4. The decision as to whether to disclose the information remains with the IC, but will be made with reference to any proposals made by the NPCC.

## 12.2. Data Subject Information Rights

12.2.1. For the purpose of either party handling information rights under Chapter III of the UK GDPR and Chapter 2 of the Data Protection Act 2018 (in respect of Shared Personal Data Processed for Civil Enforcement Purposes) or Part 3, Chapter 3 of the DPA 2018 (in respect of Shared Personal Data Processed for Criminal Enforcement Purposes), it is necessary to ensure neither party causes prejudice to the lawful activity of the other by releasing personal data disclosed by one party to the other, or indicating by the method or content of their response that such data exists. The parties agree that consultation between the parties is necessary to identify relevant prejudice and ensure it is both substantial and proportionate to the exemption which is to be applied. However, the decision to disclose or withhold the personal data (and therefore any liability arising out of that decision) remains with the party in receipt of the request as Data Controller in respect of that data.

12.2.2. A relevant request requiring consultation includes those requests exercised under the rights to access, erasure, rectification, restriction or objection which requires consideration of data provided to one party by the other.

12.2.3. Consultation will occur without undue delay and no later than 72 hours after identification of the relevant request.

12.2.4. Where the IC receives a relevant request, the IC representative is to contact the ACRO Data Protection Officer at: dataprotectionofficer@acro.police.uk to ascertain whether ACRO wishes to propose to the IC that they apply any relevant exemptions when responding to the applicant.

12.2.5. Where ACRO receives a relevant request, the ACRO Data Protection Officer is to contact the IC representatives to ascertain whether the IC wishes to propose to ACRO that they apply any relevant exemptions prior to responding to the applicant.

12.2.6. Both parties will otherwise handle such requests in accordance with the Data Protection Legislation.

12.3. **Fair processing and privacy notices**

12.3.1. Each party will take all reasonable steps to comply with the obligation to notify the data subject of the processing activity, unless an exemption applies.

12.3.2. ACRO will maintain a general notice, describing the mandatory privacy information at Articles 13 and 14 of UK GDPR and section 44(1) and (2) of the DPA 2018. ACRO will not contact the data subjects directly with this privacy information on the basis that the IC has already taken steps to inform the individual, or has exercised an appropriate exemption to Article 13 or 14, or exercised an exemption at section 44(4) of the DPA 2018.

12.3.3. The IC will take all reasonable steps to inform the data subject that checks will be conducted through ACRO, except where doing so would prejudice the purpose of the check in a way which would allow use of an exemption to this obligation. Where the IC does not provide this information to the data subject, ACRO agrees to rely upon the correct use of an exemption by the IC and will not contact the data subject to avoid the same prejudice (although ACRO expressly acknowledges that the ICO will not be responsible for ACRO's decision to place reliance on the ICO's previous reliance on a particular exemption).

# 13. Re-use of Personal Data Disclosed under this Agreement

13.1.1. Personal data shall be collected for the specified, explicit and legitimate purposes stated in this document, specifically for either the Civil Enforcement Purposes or Criminal Enforcement Purposes. Personal data cannot be further processed in a manner that is incompatible with those purposes without the written consent of the data subject that provided the information in the first instance, unless required or otherwise authorised to do so by law.

# 14. Roles and responsibilities

## 14.1. Single Point of Contact

14.1.1. ACRO and the ICO will designate SPOCs who will be responsible for ensuring the Information Sharing Agreement (ISA) is up to date and jointly solving problems relating to the sharing of information under this Agreement and act as point of first contact in the event of a suspected breach by either party.

- ACRO (UK PNC enquiries and updates):
  ACRO PNC Services Head of Section
  ****@acro.police.uk
  ****
- ICO Intelligence Department: ****
  Group Manager, Intelligence
  ****@ico.org.uk/ ****@ico.org.uk
  ****

14.1.2. Initial contact should be made by e-mail with the subject heading:
FAO ACRO/The IC ISA SPOC Ref no: XXXX

14.1.3. The above designated SPOCs will have joint responsibility of resolving all day to day operating issues and initiating the escalation process set out if/when necessary.

## 14.2. Escalation

14.2.1. In the event that the nominated SPOC cannot agree on a course of action or either party appears not to have met the terms and conditions of this Agreement, the matter should initially be referred jointly to the following:

- ACRO (UK PNC enquiries and updates):
  ACRO National Services Deputy Manager
  ****@acro.police.uk
  ****
- ACRO (Information Sharing Agreement):
  ACRO Information Management Team
  ****@acro.police.uk
  ****
- ICO Head of Intelligence: ****
  ****@ico.org.uk
  ****

14.2.2. Both ACRO and the IC SPOCs have a responsibility to create a file in which relevant information and decisions can be recorded. The file should include

details of the data accessed and notes of any correspondence, meetings attended, or phone calls made or received relating to this Agreement.

# 15. Charges

15.1. **Price and Rates**

15.1.1. The IC shall pay ACRO for the provision of services set out in this Agreement and in line with the "Letter of Charges" provided to the IC separately, which is reviewed annually.

15.2. **Invoices**

15.2.1. Invoices shall contain the following information:

- Purchase Order Number;
- The Agreement Reference Number;
- The period the service charge refers to;
- All applicable service charges;
- The name and address of both Parties (ACRO and ICO).

15.2.2. The Purchase Order Number is to be provided by the IC for the appropriate financial year to ensure payment of invoices can be made. If a Purchase Order Number is not in hand prior to receiving enquiries, ACRO reserves the right to suspend the processing of services covered under this Agreement until one has been provided.

15.2.3. The IC shall pay all monies owed to ACRO within a period of 30 days from receipt of the original invoice unless the amount shown on the invoice is disputed by the IC.

15.2.4. In the event that a financial dispute is raised by either party, this should be brought to the attention of the Chair of the NPCC in the first instance, with matters referred to the Chief Constable of the host force, HIOWC, if necessary. The Chief Finance Officer for HIOWC should be kept informed of any dispute referred to the Chair of the NPCC and/or the Chief Constable for HIOWC.

15.2.5. The equivalent IC Finance Dispute contact shall be the Director of Strategy and Planning, as the relevant budget holder.

15.2.6. If the IC is in default of this condition, ACRO reserves the right to withdraw the service by notice to the IC in writing.

# 16. Review

16.1. **Frequency**

16.1.1. This ISA will be reviewed annually, unless it meets the requirements for review under clause 20 of this Agreement.

16.1.2. This Agreement is for 2024/25.

# 17. Variation

17.1.1. No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

# 18. Waiver

18.1.1. No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

# 19. Severance

19.1.1. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Agreement.

19.1.2. If any provision or part-provision of this Agreement is deemed deleted under clause 19.1.1, the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

# 20. Changes to the applicable law

20.1.1. This Agreement documents the respective roles, processes, procedures, and agreements reached between the IC and ACRO. It should not be interpreted as removing, or reducing, existing legal obligations or responsibilities of each party, for example as Controllers under the UK GDPR and DPA. Each party agrees that it will Process the Shared Personal Data in compliance with all applicable Data Protection Legislation, laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations.

20.1.2. If during the Term the Data Protection Legislation changes in a way that the Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the SPOCs will negotiate in good faith to review the Agreement in the light of the new legislation.

## 21. No partnership or agency

21.1.1. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, make any party the agent of the other party, or authorise any party to make or enter into any commitments for or on behalf of any other party. Each party confirms it is acting on its own behalf and not for the benefit of any other person.

## 22. Notice

22.1.1. Any notice given to a party under or in connection with this Agreement shall be in writing, addressed to the SPOC and shall be:

- Delivered by hand or by pre-paid first-class post or other next working day delivery service at its principal place of business; or
- Sent by e-mail to the SPOC.

22.1.2. Notice of a cessation of services, or end to the requirement of services, will be given be either party with a period of 3 months' notice for a specified date of cessation.

22.1.3. ACRO reserves the right to give Notice of cessation with immediate affect where the IC is found to no longer have a lawful basis for requesting conviction data, is under investigation for the misuse of conviction data, or found to be in other serious breach of the Terms of this Agreement.

22.1.4. Any notice shall be deemed to have been received:

- If delivered by hand, on signature of a delivery receipt; and
- If sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second business day after posting or at the time recorded by the delivery service; and
- If sent by e-mail, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume.

22.1.5. In this clause, business hours means 9:00 am to 5:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt, and 'business day' shall be construed accordingly.

22.1.6. This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

# 23. Signature

## 23.1. **Undertaking**

23.1.1. By signing this Agreement, all signatories accept responsibility for its execution and agree to ensure that staff for whom they are responsible are trained so that requests for information and the process of sharing is sufficient to meet the purpose of this Agreement.

23.1.2. Signatories must ensure compliance with all relevant legislation.

| Signed on behalf of ACRO Senior Information Risk Owner (SIRO) | Signed on behalf of ICO |
|---|---|
| Full Name: **** | Full Name: **** |
| Position Held: CEO of ACRO | Position Held: Director of Strategy and Planning |
| Date: 19/4/24 | Date: 17/4/24 |

23.1.3. The signatory agrees the terms of this Agreement provides justified use of the Police National Computer (PNC).

| Signed as NPCC Lead Controller for PNC |
|---|
| Full Name: **** |
| Position Held:<br>NPCC Lead for PNC/LEDS- Deputy Chief Constable. |
| Date: 10.07.24 |