Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

The Information Commissioner

ACRO Criminal Records Office
enquiries@acro.pnn.police.uk | acro.police.uk

Summary Sheet

Freedom of Information Act Publication Scheme	
Security Classification (GSC)	OFFICIAL
Publication Scheme Y/N	Yes
Title	A purpose specific Information Sharing Agreement between ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO collaboration agreement, and the Information Commissioner (IC).
Version	1.0
Summary	This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for the ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO collaboration Agreement, to provide the IC with access to relevant information held on the Police National Computer (PNC), in support of the IC's regulatory and enforcement powers under the General Data Protection Regulation and the Data Protection Act 2018. Furthermore, this Agreement also allows for the recording of the details of individuals, prosecuted by the IC under the Data Protection Act, as required by the National Police Records (Recordable Offences Regulations 2000 (SI 2000/1139), onto PNC, on behalf of the IC.
Author	Information Governance Supervisor
Renewal date	26/09/2023
Date Issued	26/09/2022
ISA Reference	ACRO/042
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 42

Contents

Version control

Version No.	Date	Amendments Made	Authorisation
0.1	20/07/2020	Renewal transferred to updated template	KN, ACRO
0.2	07/09/2020	Review by IM	AAS, ACRO
0.3	14/05/2021	Updates in line with ICO requirements	KN, ACRO
0.4	18/06/2021	DPO review	KP, ACRO
0.5	09/07/2021	Updates re wording of Warranties and Indemnity Clauses	KN, ACRO
0.6	14/04/2022	ICO amendments and template updates.	KN, ACRO
0.7	14/06/2022	DPO approval of ICO amendments	KN, ACRO
0.8	23/09/2022	Reference to 'Her Majesty the Queen' amended to 'His Majesty the King' on the advice of Legal Director	AS, ICO
0.9	29/09/2022	ACRO CEO Updates	KN, ACRO
0.10	14/10/2022	Further revisions following ACRO updates/queries	AS, ICO
0.11	18/10/2022	Updates and amendments made by ACRO	AM + KN, ACRO
0.12	21/11/2022	Minor amendment, accepting ACRO changes	AS (consulting EB), ICO
1.0	24/11/2022	Annual Renewal Agreed	KN, ACRO

1. Partners to the Agreement

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

1.2. The Information Commissioner (The Commissioner)
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.

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

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, 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).

IC: Information Commissioner.

ICO: Information Commissioner's Office.

NPA: Non-Police Agency

NPPA: Non-Police Prosecuting Agency

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

Subject Information Rights: means the exercise by a data subject of his or her rights under Articles 13-22 of the UK GDPR or those rights set out in Part 3, Chapter 3 of the Data Protection Act 2018, as applicable.

Supervisory Authority: the Information Commissioner or country equivalent.

2.1.2. **Controller**, **Processor**, **Data Subject** and **Personal Data**, **Special Categories of Personal Data**, **Processing, Sensitive Processing, Personal Data Breach** 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 statue 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 UK and other countries. ACRO provides access to information held on the PNC to support the criminal justice work of some non-police prosecuting agencies; and assist safeguarding processes conducted by relevant agencies.

3.1.2. The Commissioner 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 ICO 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 Commissioner, 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 ICO. 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 the ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO collaboration agreement, to provide the Information Commissioner's Officer (ICO) with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands and final warnings. It is necessary for the ICO to have access to such information for the investigation and prosecution of offences under the Data Protection Act 2018 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. The nature of the information needed by the ICO includes both recordable and non-recordable offences.

3.2.3. Under this Agreement, the ICO 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 Data Protection Act 2018, and other recordable offences where the ICO act as the Prosecuting Agent. These will be updated on to the PNC.

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

a) Shared Personal Data is shared in a secure, confidential manner with designated points of contact;
b) Shared 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 relevant 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) Shared 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 Shared 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.

3.2.5. The parties agree to only process Shared Personal Data, (i) in the case of the ICO's discharge of its 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 Police National Computer. 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.

4. Powers

4.1. IC 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.

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 the warrant (**"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 Commissioner 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 Commissioner's Staff or an agent of the Commissioner disclosing information obtained, or provided to, the Commissioner 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.

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 is established, as a Data Processor, through the National Police Collaboration Agreement relating to the ACRO Criminal Records Office (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 and non-police prosecuting agencies.

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 Data Protection Act 2018 (DPA) the following applies;

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

4.4.5. Under section 35(3-5) and Schedule 8 of the DPA 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 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. Whereby legislation provides the organisation with a power to process Personal Data, for their 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

4.8.1. 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.

4.8.2. 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

4.9.1. 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 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 ICO, will create an Arrest Summons Number (ASN) on the PNC in relation to the impending prosecution, and will conduct PNC searches to 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 DVLA name) and alias date of births. 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 date of births. 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 ICO, for onward provision to the court, a PNC Prosecutor's and Court Multi 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 ICO Intelligence 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, 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 ICO.

5.2. PNC Searches

5.2.1. Requests for a PNC search are to be made by the ICO on a 'Names Enquiry' form, 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 ICO. This response will also indicate that 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 Intelligence 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 ICO's normal administrative procedures.

5.3.3. If required, ACRO will seek additional information from the ICO to verify the identity of the subject of the request via the following ICO mailbox:
****@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 mailbox is to be used unless this Agreement is updated to reflect a change of 'nominated' point of contact for the ICO.

5.3.6. Where appropriate, the ICO 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 a discussion would be needed, prior to any checks, in order to establish volumes and expected turnaround times. This is necessary in order to ensure ACRO can cope with the demand.

6. Submission

6.1. Names Enquiry Forms

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

6.1.2. Erroneous/incomplete 'Names Enquiry' forms will not be processed. They will be returned to the ICO as invalid and a reason provided.

6.2. Telephone Requests

6.2.1. Requests may be made by telephone in cases of emergency however 'Names Enquiry' forms must still be submitted in advance of the call. Such requests can only be made by a limited number of the ICO 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); and
- **** (Team Manager, High Priority Investigations and Intelligence).

6.2.2. The ICO may update this list by notice in writing 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 application, written or verbal, ACRO will provide a Disclosure Print to the ICO with the following information derived from the 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. PNC Warning Signals are not disclosed on Disclosure or Court Multi-prints. However, if the Commissioner wishes to confirm whether a Warning Signal is recorded on PNC for an individual that the Commissioner is investigating, then they can seek confirmation through ACRO.

7.1.4. Such requests will be completed on an ad hoc basis and will only be subject to disclosure on the basis that the Commissioner 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 Commissioner.

7.1.5. 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 Commissioner.

7.1.6. If the ICO 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

7.1.7. The ICO 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 (ASNs) 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 ICO 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 ICO 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 'NPA 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 Multi Print for each ASN created. The multi print 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 ICO 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 ICO 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 ICO, 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 ICO 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).

9.1.1. 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 partners to this Agreement will have in place baseline security measures compliant with the GMCSS. Partners are at liberty to request copies of each other's:

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

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

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

9.2.2. 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.

9.2.3. 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 the Shared Personal Data.

9.2.4. Each partner will ensure that employees or agents who have access to the Shared Personal Data have undergone appropriate data protection training, including information security training, to be competent to comply with the terms of this Agreement and the Data Protection Legislation.

9.3. Volumes

9.3.1. It is estimated that for the year 2022/23, the ICO will request up to c.120 PNC checks, and require up to c.20 PNC records to be created.

9.3.2. The ICO 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 ICO should only be made over a secure communication network i.e. TLS 1.2 e-mail encryption on the part of the ICO and an equivalent method on the part of ACRO, and care must be taken where Shared Personal Data is shared or discussed.

9.4.2. E-mails must not otherwise be password protected, contain personal data or contain 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.

9.4.4. Where e-mail transmission is unavailable, records may be transferred by post via encrypted media only. Cryptographic hardware MUST achieve a minimum of FIPS 140-2 Level 2 certification or alternatively, certification provided by the National Cyber Security Centre (NCSC).

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 was 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 section 38 of the Data Protection Act 2018, in respect of any Shared Personal Data Processed for Criminal Enforcement Purposes.

10.1.2. Where a partner rectifies Shared Personal Data, it must notify any competent authority from which the inaccurate Shared 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 Shared Personal Data 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 Shared Personal Data disclosed be disputed by the ICO or a third party, the ICO will contact ACRO to determine a suitable method to resolve the dispute.

10.3. Necessity of Shared Personal Data

10.3.1. The Commissioner 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 5 working day turnaround (not including day of receipt or response) on all cases submitted to ACRO except where ACRO requires further information from the ICO to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by the ICO.

10.4.2. Responses to requests for additional information must be made by the ICO 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 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 ICO 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 ICO. 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 NPPA form from the ICO 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 quarterly basis ACRO will 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;
- 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 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 Data Protection Act 2018 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 co-operate 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 the Shared Personal Data police data shared under this agreement must be reported immediately to the Single Points of Contact (SPOCs) designated in this Agreement.

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):

a. Contact the other party within two working days after receipt and in any event within two working days of receiving a request for information; and
b. 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 ICO 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 ICO, 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 both Chapters III of the UK GDPR and II of the Data Protection Act 2018 (in respect of Shared Personal Data Processed for Civil Enforcement Purposes) and Chapter III 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 ICO receives a relevant request the ICO representative is to contact the ACRO Data Protection Officer at: dataprotectionofficer@acro.police.uk to seek views from ACRO on any relevant exemptions which the ICO may apply when responding to the applicant.

12.2.5. Where ACRO receives a relevant request, the ACRO Data Protection Officer is to contact the ICO representatives to seek views from the ICO on any relevant exemptions which ACRO may apply when 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 to this Agreement 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 ICO 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 DPA 2018.

12.3.3. The ICO 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 ICO does not provide this information to the data subject, ACRO agrees to rely upon the correct use of an exemption by ICO 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. Personal data shall be processed for either the Civil Enforcement Purposes or Criminal Enforcement Purposes and cannot be further processed in a manner that is incompatible with those purposes, 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 work together to jointly solve 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: ****
  Intelligence Team Manager (Tactical)
  ****@ico.org.uk / ****@ico.org.uk
  ****

14.1.2. Initial contact should be made by e-mail with the subject heading:
FAO ACRO/ICO 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 Governance team
  ****@acro.police.uk
  ****

- ICO Head of Intelligence: ****
  ****@ico.org.uk
  ****

14.2.2. Both ACRO and the ICO 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, meeting attended, or phone calls made or received relating to this Agreement.

15. Charges

15.1. Price and Rates

15.1.1. The ICO shall pay ACRO for the provision of services set out in this Agreement and in line with the "Letter of Charges" provided to ICO separately and which are 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 ICO 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 ICO 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 ICO.

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, Hampshire Constabulary, if necessary. The Chief Finance Officer for Hampshire Constabulary should be kept informed of any dispute referred to the Chair of the NPCC and/or the Chief Constable for Hampshire Constabulary.

15.2.5. The equivalent ICO Finance Dispute contact shall be the Director of High Priority Inquiries, Insight, Intelligence and Relationship Management, as the relevant budget holder.

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

16. Review

16.1. Frequency

16.1.1. This ISA will be reviewed annually.

16.1.2. This Agreement makes up the annual renewal for the year 2022/23.

17. Warranties and Indemnities

17.1. Warranties

17.1.1. Each party warrants that it will:

- Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations;
- In particular, use all reasonable efforts to ensure the accuracy of any Shared Personal Data;
- Publish or otherwise make available on request a copy of this Agreement, except where a clause contains confidential information which will be redacted;
- Respond within a reasonable time and as far as reasonably possible to enquiries from the relevant Supervisory Authority in relation to the Shared Personal Data;
- Respond to Subject Access Requests in accordance with the Data Protection Legislation;
- Where applicable, pay their own appropriate fees with all relevant Supervisory Authorities to process all Shared Personal Data; and
- Take all appropriate steps to ensure compliance with the security measures set out in clause 9.2 above.

17.2. Force Majeure

17.2.1. Neither the ICO nor ACRO shall be liable to the other by reason of any failure or delay in performing its obligations under the DPA which is due to Force Majeure, where there is no practicable means available to the Party concerned to avoid such failure or delay.

17.2.2. If either the ICO or ACRO becomes aware of any circumstances of Force Majeure which give rise to any such failure or delay, or which appear likely to do so, they shall promptly give notice of those circumstances as soon as practicable after becoming aware of them and shall inform the other Party of the period for which it estimates that the failure or delay will continue.

17.2.3. For the purposes of this Condition, "Force Majeure" means any event or occurrence which is outside the control of the Party concerned and which is not attributable to any act or failure to take preventive action by the Party

concerned, but shall not include any industrial action occurring within ACRO or within any sub-contractor's organisation.

17.2.4. Any failure or delay by ACRO in performing its obligations under the DPA which results from any failure or delay by an agent, sub-contractor or supplier shall be regarded as due to Force Majeure only if that agent, sub-contractor or supplier is itself impeded in complying with an obligation to ACRO by Force Majeure.

17.3. Limitation of liability

17.3.1. Neither party excludes or limits liability to the other party for:

- Fraud or fraudulent misrepresentation;
- Death or personal injury caused by negligence;
- A breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
- Any matter for which it would be unlawful for the parties to exclude liability.

17.3.2. Subject to clause 17.3.1, neither party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

a. Any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;
b. Loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or
c. Any loss or liability (whether direct or indirect) under or in relation to any contract.

17.3.3. Clause 17.3.2 shall not prevent claims, for:

- Direct financial loss that are not excluded under any of the categories set out in clause 17.3.2(a); or
- Tangible property or physical damage.

18. Variation

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

19. Waiver

19.1. 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.

20. Severance

20.1. 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.

20.2. If any provision or part-provision of this Agreement is deemed deleted under clause 20.1 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.

21. Changes to the applicable law

21.1. 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.

22. No partnership or agency

22.1. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute 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.

23. Rights and remedies

23.1. The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

24. Notice

24.1. 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.

24.2. 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.

24.2.1. 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.

24.3. 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.

25. Governing law and Jurisdiction

25.1. This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales, and subject to the jurisdiction of the courts of England and Wales.

26. Signature

26.1. Undertaking

26.1.1. 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.

26.1.2. Parties may sign this Agreement by electronic means and agree that this method of signature is as conclusive of each party's intention to be bound by this Agreement as if signed by each party's manuscript signature. For the purposes of this Agreement, electronic means shall mean either an appropriately authorised party using a stylus or finger to sign their name, or an appropriately authorised party typing their name into the space below.

26.1.3. Signatories must ensure compliance with all relevant legislation.

Signed on behalf of ACRO Criminal Records Office	Signed on behalf of The Information Commissioner
Position Held: Chief Executive	Position Held: Director
Date: 24/11/2022	Date: 23/11/2022