Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

Office of Rail and Road (ORR)

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), as hosted by Hampshire Constabulary, acting on behalf of UK police forces that are subject to the ACRO Collaboration Agreement, and the Office of Rail and Road (ORR).
Version	2.0
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 ORR with access to relevant information held on the Police National Computer (PNC). Information will specifically relate to convictions, cautions, reprimands and final warnings for enforcement purposes in relation to prosecutions brought by ORR for recordable and non-recordable offences. Furthermore, this Agreement also allows for the recording of details on PNC of individuals prosecuted by ORR under the Health and Safety at Work Act 1974 (HSWA 1974), the REACH Enforcement Regulations 2008 and any other recordable offences where ORR act as the Prosecuting Agent.
Author	****, ACRO Information Governance Officer
Date Issued	25/01/2023
Review Date	25/10/2023
Renewal Date	25/01/2024
ISA Reference	ACRO/012
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 144

Contents

Version control

Version No.	Date	Amendments Made	Authorisation
1.0	11/08/2021	2020-21 signed ISA	KN, ACRO
1.1	29/09/2021	Initial draft version of 2021-22 agreement	AM, ACRO
1.2	05/11/2021	LBQ transfer amendments.	AM, ACRO
1.3	15/09/2022	IM review	AAS ACRO
1.4	27/09/2022	Amendments and updates following approval	AM, ACRO
1.5	25/01/2023	Suggested amendments by ORR	AM, ACRO
1.6	25/01/2023	ISA signed by ORR	RV, ORR
2.0	25/01/2023	ISA signed by ACRO CEO	JF, ACRO

1. Partners to the Agreement

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

1.2. Office of Rail and Road (ORR)
25 Cabot Square
Canary Wharf
London
E14 4QA

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.

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.

CLPD: Common Law Police Disclosure.

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: the General Data Protection Regulation as enacted into English law (**UK GDPR**) as revised and superseded from time to time; the Data Protection Act 2018 (**DPA**); and any other laws and regulations relating to the processing of Personal Data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the relevant data protection or Supervisory Authority.

DVLA: Driver and Vehicle Licensing Agency.

EARR06: Health and Safety (Enforcing Authority for Railways and Other Guided Transport Systems) Regulations 2006.

EIR: Environmental Information Regulations 2004.

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

GSCP: Government Security Classification Policy.

HSWA: Health and Safety at Work Act 1974.

ISA: Information Sharing Agreement.

NPA: Non-Police Agency.

NPCC: National Police Chiefs' Council.

NPPA: Non-Police Prosecuting Agency.

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

ORR: Office of Rail and Road.

PCC: Police and Crime Commissioner.

Personal Data means 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 2018, Article 4).

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

REACH Enforcement Regulations 2008: Registration, Evaluation, Authorisation and Restriction of Chemicals Enforcement Regulations 2008.

RSP: relevant statutory provision.

Section 22A Agreement: an Agreement is made pursuant to section 22A of the Police Act 1996 (as amended) which 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.

Special categories of Personal Data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, processing of which shall be prohibited (UK GDPR 2018, Article 9).

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.

Supervisory Authority: the Information Commissioner or country equivalent.

2.1.2. **Controller**, **Processor**, **Data Subject** and **Personal Data**, **Special Categories of Personal Data**, **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 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 Office of Rail and Road (ORR) is the independent economic and safety regulator for Britain's railways, and monitor performance and efficiency for England's Strategic Road Network.

3.1.3. ORR regulate health and safety standards and compliance across the whole rail industry and oversees competition and consumer rights issues.

3.2. Purpose

3.2.1. This Agreement sets out the framework for the sharing of Personal Data when one Controller discloses Personal Data to another Controller. 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 ORR with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands and final warnings. It is necessary for ORR to have access to such information for enforcement purposes in relation to prosecutions brought by ORR. The nature of the information needed by ORR includes both recordable and non-recordable offences.

3.2.3. Under this Agreement, ORR can request that ACRO create records on PNC for the purpose of prosecuting individuals in connection with offences listed in the HSWA 1974 and the REACH Enforcement Regulations 2008.

3.2.4. The aim of the data sharing initiative is to facilitate the statutory functions required by ORR for recordable and non-recordable offences. It will serve to benefit society by assisting ORR to carry out its law enforcement objectives with regards to investigating and prosecuting breaches of health and safety legislation. It will also ensure that PNC is up to date with the outcome of any prosecutions by the ORR.

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;
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 ORR, for the discharge of its statutory functions, and (ii) in the case of ACRO, for maintenance of centralised records on the Police National Computer (PNC). The parties shall not process Shared Personal Data in a way that is incompatible with the purposes described in this clause ("**Agreed Purpose**").

4. Powers

4.1. ORR Legal Basis

4.1.1. For the purposes of this part, "the law enforcement purposes" are the prevention, investigation, detection or prosecution of criminal penalties, including the safeguarding against threats to public safety.

4.1.2. ORR is not listed in Schedule 7 of the DPA 2018 but is a Competent Authority with a statutory function for law enforcement purposes as per section 30(1)(b) of the DPA 2018. ORR was established as a body corporate under the Railways and Transport Safety Act 2003 in place of the previous Rail Regulator.

4.1.3. The Health and Safety (Enforcing Authority for Railways and Other Guided Transport Systems) Regulations 2006 (EARR06) grants ORR the power to enforce in relation to any relevant statutory provisions (RSPs). The RSPs are defined in section 53 of the HSWA 1974 and includes Part 1 of the same Act and any other health and safety regulations. This includes the power to prosecute for breaches of any RSP under section 33 of the HSWA 1974.

4.1.4. ORR holds enforcement powers under Regulation 3 of the REACH Enforcement Regulations 2008. This allows for the investigation and prosecution of offences under Regulation 11 (offences in relation to a listed REACH provision and Schedules 4 and 5) and Regulation 13 (other offences) of the same Regulations.

4.1.5. Processing of Personal Data for any of the law enforcement purposes is lawful in that the processing is necessary for the performance of a task carried out for that purpose by a Competent Authority.

4.1.6. Processing is necessary for a law enforcement purpose and the following conditions apply as per section 35(3) to (5) and Schedule 8 (conditions for sensitive processing) of the DPA 2018;

- Statutory etc. purposes;
- Administration of Justice.

4.2. ACRO Legal Basis

4.2.1. 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.

4.2.2. ACRO is established 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 to provide PNC enquiry, update and disclosure services to non-police agencies (NPAs) and non-police prosecuting agencies (NPPAs).

4.2.3. ACRO is a competent authority, by virtue of the section 22A agreement, for processing data for a law enforcement purpose.

4.2.4. 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.

4.2.5. 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.

4.3. Code of Practice for the Management of Police Information

4.3.1. 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.

4.4. Human Rights Act 1998

4.4.1. 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.

4.4.2. 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; or
- Safeguarding the economic wellbeing of vulnerable adults.

4.5. Common Law Police Disclosure

4.5.1. Where legislation provides the organisation with a power to process Personal Data for a specific purpose, but there is no explicit legislative authority for disclosure, Common Law Police Disclosure (CLPD) 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 to do so.

4.6. 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.

4.7. 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 ORR, will create an Arrest Summons Number (ASN) on the PNC, in relation to the impending prosecutions only, 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 (not racial or ethnic origin), 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.

c) A Court/Defence/Probation PNC 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. The ORR caseworker will review all referred information and may ask for additional information to aid decision making.

5.1.4. 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 ORR.

5.2. PNC Searches

5.2.1. Requests for a PNC search are to be made by ORR 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; and
- ORR 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 ORR. 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 ORR caseworker 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 ORR's normal administrative procedures.

5.3.3. If required, ACRO will seek additional information from ORR to verify the identity of the subject of the request via the following ORR mailboxes: ****@orr.gov.uk or ****@orr.gov.uk.

5.3.4. All e-mail communication containing personal and conviction data will be exchanged using password protected WinZip files if a secure e-mail is not available.

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 ORR.

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

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 or incomplete 'Names Enquiry' forms will not be processed. They will be returned to ORR as invalid and a reason provided.

6.2. Telephone Requests

6.2.1. Requests may be made by telephone in cases of emergency however a 'Names Enquiry' form must be submitted in advance. Such requests can only be made by a limited number of ORR staff.

6.2.2. As at the date of this Agreement, ORR staff who will have the ability to make telephone requests shall be **** and ****.

6.2.3. ORR 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 application, ACRO will provide a 'Disclosure Print' to ORR 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. The exception to this is if a request is received to create or update a record held on PNC as part of a prosecution being carried out by ORR, a 'Prosecutor's and Court Multi Print' will be provided instead.

7.1.3. If ORR require an additional copy of the 'Prosecutor's and Court Multi Print' then this should be made clear in the correspondence they submit. Such requests will be charged in accordance with the letter of charges provided separately to ORR.

7.1.4. PNC Warning Signals will not be disclosed.

7.1.5. 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 ORR.

7.1.6. If ORR has a secondary query or wish 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. ORR 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. ORR 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. ORR 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 ORR is incomplete or inaccurate.

8.1.4. As part of the record creation service provided by ACRO, ORR 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. When a prosecution by ORR 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 ORR is to advise ACRO of any adjournments or disposal handed down by the court using the form, which will be supplied by ACRO separately.

8.1.6. If, once a PNC record has been created by ACRO and an ASN issued to ORR, 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), ORR 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.

9.1.2. Documents marked using the 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 of this Agreement will have in place baseline security measures compliant with or be equivalent to BS17799: 2005 and ISO/IEC 27001:2013 and HMG standards in relation to information security. Partners are at liberty to request copies of each other's:

a) Information Security Policy;
b) Records Management Policy; and
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.

9.3. Volumes

9.3.1. It is estimated that for the year 2023/24, ORR will request up to 35 PNC checks, and require up to 10 PNC records to be created.

9.3.2. ORR 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 ORR should only be made over a secure communication network, specifically the use of .gov e-mail on the part of ORR and an equivalent method on the part of ACRO, and care must be taken where personal information is shared or discussed.

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. ORR reference numbers 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, where encryption meets current industry standards.

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.

10. Information Management

10.1. Accuracy of Personal Data

10.1.1. The parties will take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay and will notify the partners to this Agreement of the erasure or rectification.

10.1.2. Where a partner rectifies 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 ORR or a third party, ORR will contact ACRO to determine a suitable method to resolve the dispute.

10.3. Turnaround

10.3.1. This Agreement requires a seven (7) 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 ORR to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by ORR.

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

10.3.3. 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.

10.3.4. An exception to the seven 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.

10.3.5. In some circumstances ORR 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 ORR. Such requests will be treated as an exception, and will be considered on a case by case basis.

10.3.6. 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 ORR in respect of every person for whom a PNC record is to be created.

10.4. Quality Assurance and Control

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

10.4.2. On a monthly basis ACRO can, if required, provide regular management information to ORR including:

- Number of PNC 'Names Enquiry' spreadsheets 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 Articles 33 and 34 of the UK GDPR 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 to provide reasonable assistance as is necessary to each other to facilitate handling of any Personal Data Breach in an expeditious and compliant manner.

11.2.3. 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.

11.2.4. 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.

11.2.5. 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 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 another partner, 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 ORR 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 ORR, 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 UK GDPR and Part 3, Chapter 3 of the DPA 2018, 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.

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 provide 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 ORR receives a relevant request, the ORR Data Protection Officer is to contact the ACRO Data Protection Officer at: dataprotectionofficer@acro.police.uk to ascertain whether ACRO wishes to propose to ORR 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 ORR Data Protection Officer at: dpo@orr.gov.uk to ascertain whether ORR 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 partner 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 ORR 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. ORR 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 ORR does not provide this information to the data subject, ACRO agrees to rely upon the correct use of an exemption by ORR and will not contact the data subject to avoid the same prejudice.

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

13.1. Personal Data shall be collected for the specified, explicit and legitimate purposes stated in this document and 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 to by law.

14. Roles and responsibilities

14.1. Single points of contact

14.1.1. ACRO and ORR 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
  ****

- Office of Rail and Road
  **** – Litigation Officer, Railway Safety Directorate
  ****@orr.gov.uk

14.1.2. Initial contact should be made by e-mail with the subject heading:
FAO ACRO/ORR 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
  ****

- Office of Rail and Road
  **** - Legal Business and Litigation Manager
  ****@orr.gov.uk

14.2.2. Both the ACRO and ORR 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. ORR shall pay ACRO for the provision of services set out in this Agreement and in line with the "Letter of Charges" provided to ORR 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; and
- The name and address of both Parties (ACRO and ORR).

15.2.2. The Purchase Order Number is to be provided by ORR 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. ORR 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 ORR.

15.2.4. If ORR 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 is reviewed annually. This is the 2023/24 Agreement.

16.1.2. This ISA will be reviewed nine months after implementation and expire after one year and a renewal agreement put in place.

16.1.3. ACRO Information Management will conduct a review ahead of an Agreement renewal, offering ORR the opportunity to provide service feedback. Renewal of the Agreement will be subject to the review findings.

16.1.4. Renewal documentation will be created between the review and expiry dates of this Agreement, with a new Agreement to be established in line with the expiry to support continuation of service.

16.1.5. Where a renewed Agreement cannot be established in time for this Agreement's expiry, an Extension Letter will be issued by ACRO to confirm that requests, and services, will be conducted under the Terms and Conditions of the most recent Agreement. Both parties must sign to this letter of extension to confirm this approach.

17. Warranties and Indemnities

17.1. Warranties

17.1.1. Each party warrants and undertakes 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 Personal Data shared;
- 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 for the Agreed Purpose; and
- Take all appropriate steps to ensure compliance with the security measures set out in clause 9.2.2 above.

17.2. Indemnity

17.2.1. The parties undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this Agreement, except to the extent that any such liability is excluded under clause 17.3.2.

17.2.2. Indemnification hereunder is contingent upon:

- The party to be indemnified (the **indemnified party**) promptly notifying the other party (the **indemnifying party**) of a claim;
- The indemnifying party having sole control of the defence and settlement of any such claim; and
- The indemnified party providing reasonable co-operation and assistance to the indemnifying party in defence of such claim.

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, 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.

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. Signatories must ensure compliance with all relevant legislation.

Signed on behalf of ACRO Criminal Records Office	Signed on behalf of the Office of Rail and Road
Position Held: Chief Executive	Position Held: Investigation and Enforcement Manager
Date: 25/01/2023	Date: 25/01/2023