

OFFICIAL

ACRO

Criminal Records Office

Information Sharing Agreement

Between

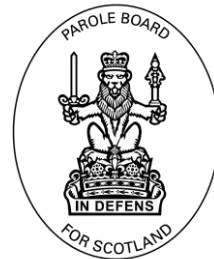
**National Police Chiefs' Council
ACRO Criminal Records Office**

And

Parole Board for Scotland



ACRO Criminal Records Office



ACRO Criminal Records Office

enquiries@acro.police.uk | acro.police.uk

Summary Sheet

| Freedom of Information Act Publication Scheme | |
|--|---|
| Security Classification (GSC) | OFFICIAL |
| Publication Scheme Y/N | Yes |
| Title | Information Sharing Agreement between ACRO Criminal Records Office (ACRO) and the Parole Board for Scotland (PBS) |
| Version | 1.0 |
| Summary | <p>This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for the ACRO, acting on behalf of UK police forces that are subject to the ACRO section 22A Collaboration Agreement, to provide PBS with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands and final warnings for the purpose of carrying out risk assessment and risk management of offenders due for parole.</p> <p>Under this Agreement, PBS can request criminal conviction information held outside of the UK via ACRO when there is a lawful basis to do so.</p> |
| Author | **** Development Officer |
| Date Issued | 01/05/2024 |
| Review date | 01/02/2025 |
| Expiry date | 01/05/2025 |
| ISA Reference | ACRO/208 |
| Location of Agreement | ACRO ISA Library |
| ACRO DPIA Reference | DPIA 208 |

Contents

| | |
|--|----|
| Summary Sheet | 2 |
| Version control..... | 5 |
| 1. Partners to the Agreement | 6 |
| 2. Agreed Terms | 7 |
| 2.1. Interpretation | 7 |
| 3. Purpose and background of the Agreement | 10 |
| 3.1. Background | 10 |
| 3.2. Purpose | 10 |
| 4. Powers..... | 11 |
| 4.1. PBS Legal Basis | 11 |
| 4.2. ACRO Legal Basis | 12 |
| 4.3. Code of Practice for the Management of Police Information | 12 |
| 4.4. Human Rights Act 1998..... | 13 |
| 4.5. Common Law Police Disclosure | 13 |
| 4.6. Crime and Disorder Act 1998 | 13 |
| 4.7. The Policing Protocol Order 2011 | 13 |
| 5. Process | 14 |
| 5.1. Overview | 14 |
| 5.2. PNC Searches | 14 |
| 5.3. Additional Information Requirements | 15 |
| 6. Submission | 15 |
| 6.1. Names Enquiry Spreadsheets | 15 |
| 6.2. Telephone Requests..... | 15 |
| 7. Provision of Information | 16 |
| 7.1. Response to a PNC Names Enquiry Search | 16 |
| 8. International Requests..... | 16 |
| 8.1. Process | 16 |
| 8.2. Exchange of Criminal Records with the EU | 17 |
| 8.3. Exchange of Criminal Records with Non-EU Countries | 17 |
| 8.4. Specific Data Handling | 18 |
| 9. Information Security | 18 |
| 9.1. Government Security Classification Policy..... | 18 |
| 9.2. Security Standards | 18 |
| 9.3. Volumes | 19 |
| 9.4. Transmission | 19 |

OFFICIAL

| | | |
|-------|--|----|
| 9.5. | Retention and disposal | 20 |
| 10. | Information Management | 20 |
| 10.1. | Accuracy of Personal Data | 20 |
| 10.2. | Accuracy Disputes | 20 |
| 10.3. | Turnaround | 20 |
| 10.4. | Quality Assurance and Control | 21 |
| 11. | Complaints and Breaches | 22 |
| 11.1. | Complaints | 22 |
| 11.2. | Breaches..... | 22 |
| 12. | Information Rights | 23 |
| 12.1. | Freedom of Information Act 2000 | 23 |
| 12.2. | Data Subject Information Rights | 23 |
| 12.3. | Fair processing and privacy notices | 24 |
| 13. | Re-use of Personal Data Disclosed under this Agreement | 24 |
| 14. | Roles and responsibilities | 25 |
| 14.1. | Single Point of Contact..... | 25 |
| 14.2. | Escalation | 25 |
| 15. | Charges..... | 26 |
| 15.1. | Price and Rates..... | 26 |
| 15.2. | Invoices | 26 |
| 16. | Review..... | 27 |
| 16.1. | Frequency | 27 |
| 17. | Variation..... | 27 |
| 18. | Waiver | 27 |
| 19. | Severance..... | 27 |
| 20. | Changes to the applicable law | 27 |
| 21. | No partnership or agency | 27 |
| 22. | Notice..... | 28 |
| 23. | Signature | 29 |
| 23.1. | Undertaking | 29 |

Version control

| Version No. | Date | Amendments Made | Authorisation |
|--------------------|-------------|------------------------------------|----------------------|
| 0.1 | 06/07/2023 | Initial Draft | 17501 |
| 0.2 | 02/10/2023 | IM Review | 14258 |
| 0.3 | 06/10/2023 | DPO Review | 16715 |
| 0.4 | 13/02/2024 | Signed PBS | 17501 |
| 0.5 | 28/03/2024 | ACRO CEO sign off | 17501 |
| 1.0 | 21/05/2024 | PNC Lead sign off and finalisation | 17501 |

1. Partners to the Agreement

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

1.2. Parole Board for Scotland
X Spur, Saughton House
Broomhouse Drive
Edinburgh
EH11 3XD

ICO Registration Number Z7574031

2. Agreed Terms

2.1. Interpretation

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

2.1.1. Definitions:

ACRO: ACRO Criminal Records Office.

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

ASN: Arrest Summons Number

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

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

CEO: Chief Executive Officer

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 2018**); 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.

DCC: Deputy Chief Constable

EIR: Environmental Information Regulations 2004.

EU: European Union

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

GSCP: Government Security Classification Policy.

MB: Megabyte (of data)

NFA: No Further Action

NPA: Non-Police Agency.

NPCC: National Police Chiefs' Council.

NPPA: Non-Police Prosecuting Agency.

OCiP: Operational Communications in Policing

OIC: Officer in charge of the case

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

PACE: Police and Criminal Evidence Act 1984

PBS: Parole Board for Scotland

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, 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.

PNC: Police National Computer

PND: Police National Database

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

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

SIRO: Senior Information Risk Owner.

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, 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 or sections 45 to 49 of the DPA 2018.

Supervisory Authority: the Information Commissioner or country equivalent.

UK: United Kingdom

WinZip: trialware file archiver and compressor for Microsoft Windows

- 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 statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
- 2.1.6. Any words following the terms **including, include, in particular or for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.
- 2.1.7. A reference to **writing** or **written** includes e-mail.
- 2.1.8. Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.

3. Purpose and background of the Agreement

3.1. Background

- 3.1.1. ACRO, hosted by HIOWC, 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 (NPPAs) and assists safeguarding processes conducted by relevant agencies.
- 3.1.2. PBS is a Tribunal non-departmental public body. The Board is a judicial body which is independent of the Scottish Government and impartial in its duties. Its main aim is to ensure that those prisoners who are no longer regarded as presenting a risk to public safety may serve the remainder of their sentence in the community on licence under the supervision of a supervising officer.

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 ACRO Criminal Records Office (ACRO), acting on behalf of UK police forces that are subject to the ACRO section 22A Collaboration Agreement, to provide the PBS with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands and final warnings. It is necessary for the PBS to have access to such information for fully assessing the risk posed by a person that may serve the remainder of their sentence in the community. The nature of the information required by the PBS includes both recordable and non-recordable offences.
- 3.2.3. Under this Agreement, PBS can request criminal conviction information held outside of the UK via ACRO when there is a lawful basis to do so.
- 3.2.4. The aim of the data sharing initiative is to supply information required by PBS for recordable and non-recordable offences. It will serve to benefit society by protecting the public.
- 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 the PBS to discharge its statutory functions, and (ii) in the case of ACRO, for maintenance of centralised records on the PNC. The parties shall not process Shared Personal Data in a way that is incompatible with the purposes described in this clause ("**Agreed Purpose**").

4. Powers

4.1. PBS Legal Basis

- 4.1.1. For the purposes of this part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety.
- 4.1.2. The PBS exists under the provisions of the Prisons (Scotland) Act 1989, the Prisoners and Criminal Proceedings (Scotland) Act 1993, the Convention Rights (Compliance) (Scotland) Act 2001 and the Criminal Justice (Scotland) Act 2003. and as such are a Competent Authority under Schedule 7 of the Data Protection Act (DPA) 2018.
- 4.1.3. 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.
- 4.1.4. Processing is necessary for a law enforcement purpose and the following conditions apply as per section 35(3) to 35(5) and Schedule 8 (conditions for sensitive processing) of the DPA 2018);
 - Statutory etc. purposes;
 - Administration of justice;
 - Protecting individual's vital interests
 - Safeguarding of children and of individuals at risk
 - Judicial Acts

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, hosted by HIOWC, is established through the National Police Collaboration Agreement relating to ACRO under section 22A of the Police Act 1996. This Agreement gives ACRO the authority to act on behalf of the Chief Constables to provide PNC enquiry, update and disclosure services to NPAs) and NPPAs.
- 4.2.3. ACRO is a Competent Authority, by virtue of the section 22A Agreement, 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.
- 4.2.6. ACRO have been delegated responsibility for managing the UK Central Authority for the Exchange of Criminal Records (UKCA-ECR). As such, ACRO discharge the UK's responsibilities under the 1959 Convention on Mutual Assistance in Criminal Matters and the Trade and Co-operation Agreement between the European Union and the United Kingdom, Part 3, Title IX on the exchange of information extracted from the criminal record.
- 4.2.7. ACRO also exchange conviction information with countries outside of the EU via Interpol channels, subject to Interpol Protocols.

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;
- 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, 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.

4.6. 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 the PBS will conduct PNC searches and provide a PNC print to meet their information needs.
- 5.1.2. The PNC data will comprise of:
- a) A Disclosure PNC print. The personal data disclosed under this print includes (if available): name, date of birth, birth place, sex, address, occupation, aliases (including Driver and Vehicle Licensing Agency (DVLA) name) and alias dates of birth. The home address that is printed in the ID part of the print is decided by the following rules:
 - If there is more than one home address on the record, the most recent address is used;
 - If there is no home address present, the most recent 'no fixed abode' address type will be used;
 - If neither of the above address types are present, the most recent 'Other' address is printed.
- 5.1.3. The PBS caseworker will review all referred information and may ask for additional information to aid decision making.

5.2. PNC Searches

- 5.2.1. Requests for a PNC search are to be made by the PBS 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;
 - PBS 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 PBS. 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 PBS 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 the PBS normal administrative procedures.
- 5.3.3. If required, ACRO will seek additional information from the PBS to verify the identity of the subject of the request via the following PBS mailbox: ****@paroleboard.scot
- 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 mailbox is to be used unless this Agreement is updated to reflect a change of 'nominated' point of contact for the PBS.
- 5.3.6. Where appropriate, the PBS will make contact with the subject of the enquiry to seek the additional information required by ACRO.

6. Submission

6.1. Names Enquiry Spreadsheets

- 6.1.1. Completed 'Names Enquiry' spreadsheets are to be sent via secure e-mail to the following e-mail address: ****@acro.police.uk
- 6.1.2. ACRO will receive requests from PBS, via the following secure mailbox: ****@paroleboard.scot
- 6.1.3. Erroneous or incomplete 'Names Enquiry' spreadsheets will not be processed. They will be returned to the PBS as invalid and a reason provided.

6.2. Telephone Requests

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

- 6.2.2. Such requests can only be made by a limited number of the PBS staff. As at the date of this Agreement, the PBS staff who will have the ability to make telephone requests shall **** and ****.
- 6.2.3. The PBS may update this list by notice to ACRO from time to time.

7. Provision of Information

7.1. Response to a PNC Names Enquiry Search

- 7.1.1. In response to a formal written application, ACRO will provide a Disclosure Print to the PBS 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 PBS.
- 7.1.3. PBS 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
- 7.1.4. The PBS 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. International Requests

8.1. Process

- 8.1.1. If the subject of a parole risk assessment is a foreign national, a request may be made via the International Services team at ACRO to obtain, if available, details of the subject's conviction history in his/her country of nationality.
- 8.1.2. The purpose of this process is to enable the subject's full criminal history to be made available in order to effectively assess the individual's eligibility to be considered for parole.
- 8.1.3. ACRO can submit requests to EU and non-EU countries for criminal conviction information. The process of this is detailed in clauses 8.2 and 8.3.

- 8.1.4. Requests should be made using the International Request form which will be supplied by ACRO separately; and sent, one request per e-mail, from the nominated PBS mailbox to the ACRO International Requests Mailbox: ****@acro.police.uk. Erroneous or incomplete forms may delay the processing of the request.
- 8.1.5. ACRO will forward the request to the relevant national authority/ies for a response as per the instances set out in clauses 8.2 and 8.3.
- 8.1.6. Requests may be rejected if there is insufficient information to enable the receiving country to verify the identity of the subject, or if the mandatory nominal information is not supplied. Requests may not be sent if the destination country does not have a criminal register or is categorised as an extreme/severe risk country. Guidance on the required information will be sent to the PBS separately, and ACRO will send updated copies if this information changes.
- 8.1.7. Once a response has been received from the country of nationality, ACRO shall forward the conviction/non-conviction information, including any necessary translation, to the nominated PBS mailbox. If this mailbox is not .pnn, .gsi or .cjsm secure, then additional security protections may be required.

8.2. Exchange of Criminal Records with the EU

- 8.2.1. If the subject is an EU national, then ACRO shall deal with the request under the 1959 Convention on Mutual Assistance in Criminal Matters and the EU-UK Trade Co-operation agreement between the European Union and the United Kingdom, Part 3, Title IX on the exchange of information extracted from the criminal record.
- 8.2.2. There is a mandated response time of 20 working days for the requested country to respond in criminal proceedings only. As requests made under this Agreement will be for non-criminal proceedings there is no mandated timescale for countries to respond.
- 8.2.3. ACRO shall forward the information as soon as possible after it has been received from the requesting country and any necessary translation has taken place.
- 8.2.4. Requests made outside of criminal proceedings may not be responded to, and are subject to legislation and processes in the requesting country. Guidance on which countries will respond to requests outside of criminal proceedings will be provided to the PBS by ACRO.

8.3. Exchange of Criminal Records with Non-EU Countries

- 8.3.1. If the subject is a non-EU national, a request shall be submitted through Interpol to the destination country.

8.3.2. Under Interpol protocols, countries are not mandated to respond to requests for criminal conviction information. Therefore ACRO are unable to provide a turnaround time for responses or guarantee a response will be received.

8.3.3. ACRO shall forward the information as soon as possible after it has been received from the requesting country and any necessary translation has taken place.

8.4. Specific Data Handling

8.4.1. Any conviction information that is supplied by ACRO with regards to foreign convictions cannot be held on any system outside of ACRO/PBS ownership (such as local information systems) and can only be used for the purposes (i.e. the specific case) for which it was requested.

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 OFFICIAL – SENSITIVE, in which case specific handling conditions will be provided.

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

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

9.2. Security Standards

9.2.1. It is expected that partners to this Agreement will have in place baseline security measures compliant with or 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;
- 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 2023/2024, the PBS will request up to 25 PNC Checks and 10 International Requests.
- 9.3.2. The PBS will advise ACRO if the number of PNC Checks/International Requests 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 PBS should only be made over a secure communication network email on the part of the PBS 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. The PBS 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, 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 the PBS or a third party, the PBS will contact ACRO to determine a suitable method to resolve the dispute.

10.3. Turnaround

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

- 10.3.2. For turnaround times for International Requests please see clause 8.2.2 of this Agreement.
- 10.3.3. Responses to requests for additional information must be made by the PBS within 10 working days (not including day of receipt or response). If ACRO do not receive the information, the request will be closed.
- 10.3.4. 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.
- 10.3.5. An exception to the 7 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.
- 10.3.6. In some circumstances the PBS 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 PBS. Such requests will be treated as an exception, and will be considered on a case by case basis.

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 the PBS including:
- Number of PNC 'Names Enquiry' forms received
 - Number of PNC Disclosure Prints provided
 - Number of International Requests
 - 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 the 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 cooperate 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 document.

12. Information Rights

12.1. Freedom of Information Act 2000

- 12.1.1. Where a party to this Agreement is subject to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) all parties shall assist and co-operate with the other to enable the other party to comply with its obligations under FOIA and the EIR. This is in line with the requirements laid out in the Lord Chancellor's Code of Practice issued under section 45 of FOIA.
- 12.1.2. Where a party receives a request for information in relation to information which it received from the other party, it shall (and will ensure that any sub-contractors it procures shall also):
- Contact the other party within two working days after receipt and in any event within two working days of receiving a request for information;
 - The originating authority will provide all necessary assistance as reasonably requested by the party to enable the other party to respond to a request for information within the time for compliance set out in section 10 of the FOIA or Regulation 5 of the EIR.
- 12.1.3. On receipt of a request made under the provisions of the FOIA in respect of information provided by or relating to the information provided by ACRO, the PBS 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 PBS, but will be made with reference to any proposals made by the NPCC.

12.2. Data Subject Information Rights

- 12.2.1. For the purpose of either party handling information rights under Chapter III of the UK GDPR or 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 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 PBS receives a relevant request, the PBS representative is to contact the ACRO Data Protection Officer at: dataprotectionofficer@acro.police.uk to ascertain whether ACRO wishes to propose to the PBS 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 PBS representatives to ascertain whether PBS wishes to propose to ACRO that they apply any relevant exemptions prior to responding to the applicant.
- 12.2.6. Both parties will otherwise handle such requests in accordance with the Data Protection Legislation.

12.3. Fair processing and privacy notices

- 12.3.1. Each party will take all reasonable steps to comply with the obligation to notify the data subject of the processing activity, unless an exemption applies.
- 12.3.2. ACRO will maintain a general notice, describing the mandatory privacy information at Articles 13 and 14 of UK GDPR and section 44(1) and (2) of the DPA 2018. ACRO will not contact the data subjects directly with this privacy information on the basis that PBS has already taken steps to inform the individual, or has exercised an appropriate exemption to Article 13 or 14, or exercised an exemption at section 44(4) of the DPA 2018.
- 12.3.3. The PBS 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 PBS does not provide this information to the data subject, ACRO agrees to rely upon the correct use of an exemption by PBS 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 Point of Contact

14.1.1. ACRO and the PBS 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

- ACRO (International requests):
ACRO International Services Head of Section
****@acro.police.uk

- PBS: - Corporate Services
**** (DPO)
****@paroleboard.scot

14.1.2. Initial contact should be made by e-mail with the subject heading:
FAO ACRO/ PBS 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 (International requests):
ACRO International Services Deputy Manager
****@acro.police.uk

- ACRO (Information Sharing Agreement):
ACRO Information Management Team
****@acro.police.uk

- PBS: Corporate Services
**** (Head of Corporate Services)
****@paroleboard.scot

- 14.2.2. Both ACRO and the PBS SPOCs have a responsibility to create a file in which relevant information and decisions can be recorded. The file should include details of the data accessed and notes of any correspondence, meetings attended, or phone calls made or received relating to this Agreement.

15. Charges

15.1. Price and Rates

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

15.2. Invoices

- 15.2.1. Invoices shall contain the following information:
- Purchase Order Number;
 - The Agreement Reference Number;
 - The period the service charge refers to;
 - All applicable service charges;
 - The name and address of both Parties (ACRO and PBS).
- 15.2.2. The Purchase Order Number is to be provided by the PBS 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 PBS 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 PBS.
- 15.2.4. If the PBS 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 is for 2023/24.

17. Variation

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

18. Waiver

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

19. Severance

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

19.2. If any provision or part-provision of this Agreement is deemed deleted under clause 19.1 the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

20. Changes to the applicable law

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

21. No partnership or agency

21.1. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, make any party the agent of the other party, or authorise any party to make or enter into any

commitments for or on behalf of any other party. Each party confirms it is acting on its own behalf and not for the benefit of any other person.

22. Notice

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

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

22.2. 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.

22.2.1. 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.

22.3. 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.

23. Signature

23.1. Undertaking

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

23.1.2. Signatories must ensure compliance with all relevant legislation.

| | |
|---|---------------------------------------|
| Signed on behalf of ACRO Senior Information Risk Owner (SIRO) | Signed on behalf of PBS |
| Full Name: **** | Full Name: **** |
| Position Held: CEO of ACRO | Position Held: CEO OF PAROLE SCOTLAND |
| Date: 25 th March 2024 | Date: 13/02/2024 |

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

| |
|--|
| Signed as NPCC Lead Controller for PNC |
| Full Name: **** |
| Position Held: Deputy Chief Constable, NPCC lead for PNC/LEDS |
| Date: 01.05.2024 |