ACRO
Criminal Records Office

Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

Serious Fraud Office (Security Checks) (SFO-SC)

NPCC
National Police Chiefs' Council
ACRO Criminal Records Office

SERIOUS
FRAUD OFFICE

Summary Sheet

Freedom of Information Act Publication Scheme	
Security Classification (GSC)	OFFICIAL
Publication Scheme Y/N	Yes
Title	A purpose specific Information Sharing Agreement between ACRO Criminal Records Office (ACRO), acting on behalf of the National Police Chiefs' Council (NPCC), and Serious Fraud Office (Security Checks) (SFO-SC).
Version	1.0
Summary	*Services* This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for the ACRO Criminal Records Office (ACRO), acting on behalf of the National Police Chiefs' Council (NPCC), to provide Serious Fraud Office (Security Checks) (SFO-SC) with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands and final warnings for enforcement purposes in relation to prosecutions brought by the SFO-SC for recordable and non-recordable offences.
Author	Records Management Supervisor
Review Date	08/07/2020
Date Issued	09/07/2019
ISA Ref	ACRO/010
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 004

Contents

Version Record

Version No.	Date	Amendments Made	Authorisation
1.0	*06/06/2019*	*Annual Renewal, numerous amendments due to changes in process, GDPR and DPA 2018*	*AMB, ACRO*

1. Partners to the Agreement

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

1.2. Serious Fraud Office (Security Checks) (SFO-SC)
2-4 Cockspur Street
London
SW1Y 5BS

2. Purpose and Background of the Agreement

2.1. Purpose

2.1.1. The purpose of this Agreement is to formalise the arrangements for the ACRO Criminal Records Office (ACRO), acting on behalf of the National Police Chiefs' Council (NPCC), to provide Serious Fraud Office (Security Checks) (SFO-SC) with access to relevant information held on the Police National Computer (PNC), specifically convictions, adult cautions, youth cautions, reprimands and final warnings for enforcement purposes in relation to prosecutions brought by SFO-SC for recordable offences (and non-recordable offences where they are recorded on PNC).

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

- Information is shared in a secure, confidential manner with designated points of contact
- Information is shared only on a 'need to know' basis
- There are clear procedures to be followed with regard to information sharing
- Information will only be used for the reason(s) it has been obtained
- Data quality is maintained and errors are rectified without undue delay
- Lawful and necessary reuse does not compromise either party, and
- Subject information rights are observed without undue prejudice to the lawful purpose of either party

2.2. Background

2.2.1. ACRO is a national police unit under the NPCC working for safer communities. 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.

2.2.2. ACRO is the national police unit responsible for exchanging criminal conviction information between the UK and other countries.

2.2.3. The Serious Fraud Office is an independent Government department, operating under the superintendence of the Attorney General. Its Purpose is to protect society by investigating and, if appropriate, prosecuting those who commit serious or complex fraud, bribery and corruption and pursuing them and others for the proceeds of their crime.

3. Powers

3.1. SFO-SC Legal Basis

3.1.1. The SFO-SC was established under Criminal Justice Act 1987. The function of the SFO-SC is to investigate and/or prosecute offences under the Criminal Justice Act 1987 in particular section 1(3)-(5). It is a competent authority for the purposes of law enforcement processing to the extent of these powers.

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

3.1.3. The SFO-SC investigations and prosecutions activities are concerned with the following offences:

- Section 1(3)-(5) - Serious or complex fraud (a term which also encompasses serious or complex offences of bribery or corruption offences)

3.1.4. The SFO-SC is permitted to process special category personal data for preventing or detecting unlawful acts when strictly necessary to meet the purpose and when the processing conditions of schedule 8 of the DPA 2018 are met. The condition(s) used for this agreement are:

- A function conferred by under any rule of law, necessary in the substantial public interest
- Anti-fraud organisations
- Archiving, Statistics, Research

3.2. ACRO Legal Basis

3.2.1. 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.

3.2.2. 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 and non-police prosecuting agencies.

3.3. Code of Practice for the Management of Police Information

3.3.1. This agreement outlines the need for the Police and Partners to work together to share information in line with the Policing Purpose 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;
- Any duty or responsibility of the police arising from common or statute law.

3.4. Human Rights Act 1998

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

3.4.2. Interference with this right may be justified where lawful and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Lawful intrusion by the police service requires proportionate use of personal data for any of the policing purposes.

3.5. Common Law Duty of Confidentiality

3.5.1. This Agreement takes into account the common law duty of confidentiality which applies where information has a necessary quality of confidence or where information is imparted in circumstances giving rise to an obligation of confidence that is either explicit or implied. Where the duty applies, disclosure will be justified only by:

- consent
- a legal duty
- a public interest through consent, legal duty and the public interest or for the safeguarding of one or more people.

4. Process

4.1. Overview

4.1.1. ACRO, in response to requests made by the SFO-SC, will conduct PNC searches and provide a PNC print to meet the information needs of SFO-SC.

4.1.2. The PNC data will comprise of:

- A Disclosure PNC print. The personal data disclosed under this print includes (if available): name, date of birth, birth place, sex (not colour), address, occupation, aliases (including DVLA name) and alias date of births. The home address that is printed in the ID part of the print is decided by the following rules:
  - If there is more than one home address on the record, the most recent address is used,
  - If there is no home address present, the most recent 'no fixed abode' address type will be used,
  - If neither of the above address types are present, the most recent 'Other' address is printed.
- A Prosecutors 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 date of births. The home address that is printed in the ID part of the print is decided by the following rules:
  - If there is more than one home address on the record, the most recent address is used,
  - If there is no home address present, the most recent 'no fixed abode' address type will be used,
  - If neither of the above address types are present, the most recent 'Other' address is printed.
- 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 date of births. The home address that is printed in the ID part of the print is decided by the following rules:
  - If there is more than one home address on the record, the most recent address is used,
  - If there is no home address present, the most recent 'no fixed abode' address type will be used,
  - If neither of the above address types are present, the most recent 'Other' address is printed.

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

4.1.4. 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 SFO-SC. This response will also indicate that in the absence

of fingerprints the identity of the subject cannot be verified. Similar wording will apply to 'Trace' returns i.e. when a record is found and a PNC print provided.

4.1.5. The SFO-SC caseworker will review all referred information and may ask for additional information to aid decision making.

4.2. PNC Searches

4.2.1. Requests for a PNC search are to be made by the SFO-SC on a 'Names Enquiry' form which will be supplied by ACRO separately.

4.2.2. The following personal data[1] is to be provided in support of each request:

- First name
- Any middle names
- Surname / family name
- Date of Birth (dd/mm/yyyy)
- Any alias details (names, DoB)
- Place of birth (where known)
- Address
- SFO-SC case reference

4.3. Additional Information Requirements

4.3.1. Other personal data which the SFO-SC 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.

4.3.2. 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 SFO-SC normal administrative procedures.

4.3.3. If required, ACRO will seek additional information from the SFO-SC to verify the identity of the subject of the request via the following secure SFO-SC mailbox:
****

4.3.4. No other mailbox is to be used unless this Agreement is updated to reflect a change of 'nominated' point of contact for the SFO-SC.

4.3.5. Where appropriate, the SFO-SC will make contact with the subject of the enquiry to seek the additional information required by ACRO.

[1] Personal data is defined by Data Protection Legislation as information that relates to an identified or identifiable individual.

5. Submission

5.1. Names Enquiry Forms

5.1.1. Completed 'Names Enquiry' forms are to be sent via secure email to the following email address:
****

5.1.2. Erroneous/incomplete 'Names Enquiry' forms will not be processed. They will be returned to the SFO-SC as invalid and a reason provided.

5.2. Telephone Requests

5.2.1. Requests may be made by telephone in cases of emergency and 'Names Enquiry' form submitted retrospectively. Such requests can only be made by a limited number of the SFO-SC staff.

6. Provision of Information

6.1. Response to a PNC 'Names' Search

6.1.1. In response to a formal application, written or verbal, ACRO will provide a Disclosure Print to the SFO-SC 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).

6.1.2. 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 SFO-SC. A disclosure print will be supplied by ACRO separately.

If the SFO-SC 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:
****

6.1.3. The SFO-SC will need to liaise directly with forces to explain 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.

7. Information Security

7.1. Government Security Classification Policy

7.1.1. 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.

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

- Any specific limitations on dissemination, circulation or intended audience
- Any exception to consult should reuse be anticipated
- Additional secure handling and disposal requirements

7.2. Security Standards

7.2.1. 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:

- Information Security Policy
- Records Management Policy
- Data Protection Policy

7.2.2. Each partner will implement and maintain appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss or destruction of, or damage.

7.2.3. 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.

7.3. Volumes

7.3.1. Is it estimated that for the year 2019-20, the SFO-SC will request c500 PNC checks.

7.3.2. The SFO-SC will advise ACRO if the number of PNC checks is likely to be exceeded.

7.3.3. 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.

7.4. Transmission

7.4.1. With the exception of telephone requests in cases of emergency, contact between ACRO and the SFO-SC should only be made over a secure communication network and care must be taken where personal information is shared or discussed.

7.4.2. Emails must not be password protected, contain personal data or contain the descriptor 'Private and Confidential' in subject field, or be over 6MB in file size.

7.4.3. The SFO-SC reference number must be included in the subject field of every email sent to ACRO.

7.4.4. Where email transmission is unavailable, records may be transferred by post via encrypted disk, where encryption meets current industry standards.

7.5. Retention and disposal

7.5.1. Information shared under this Agreement will be securely stored and disposed 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.

8. Information Management

8.1. Accuracy of Personal Data

8.1.1. 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.

8.1.2. 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 of the correction, unless a compelling reason for not doing so exists.

8.1.3. 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.

8.2. Accuracy Disputes

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

8.3. Turnaround

8.3.1. This Agreement requires a 7 working day turnaround on all cases submitted to ACRO except where ACRO requires further information from the SFO-SC to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by the SFO-SC.

8.3.2. Responses to requests for additional information must be made by the SFO-SC within 10 working days. If ACRO do not receive the information, the request will be closed.

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

8.3.4. 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.

8.3.5. In some circumstances the SFO-SC 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 SFO-SC. Such requests will be treated as an exception, and will considered on a case by case basis.

8.4. Quality Assurance and Control

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

8.4.2. On a monthly basis ACRO can, if required, provide regular management information to the SFO-SC including:

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

9. Complaints and Breaches

9.1. Complaints

9.1.1. 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 the other parties where appropriate.

9.2. Breaches

9.2.1. Should information shared under this agreement be disclosed outside of this agreement, lost or stolen, then it will be the responsibility of the respective data controller to report this immediately and to follow their security incident reporting procedures.

9.2.2. All security incidents and breaches involving police data shared under this agreement must be reported immediately to the SPOCs designated in this agreement.

10. Information Rights

10.1. Freedom of Information Act 2000

10.1.1. 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.

10.1.2. Where a party receives a request for information in relation to the information which it received from another party, it shall (and shall procure that its sub-contractors shall):

- Contact the other party within two working days after receipt and in any event within two working days 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.

10.1.3. On receipt of a request made under the provisions of the Freedom of Information Act 2000 in respect of information provided by or relating to the information provided by ACRO, the SFO-SC representatives is to ascertain whether the NPCC wishes to propose the engagement of any exemptions via the NPCC FOI mailbox: npcc.foi.request@cru.pnn.police.uk

10.1.4. The decision as to whether to disclose the information remains with SFO-SC, but will be made with reference to any proposals made by the NPCC.

10.2. Data Subject Information Rights

10.2.1. For the purpose of either party handling information rights under Chapter III of both the DPA 2018 and GDPR, it is necessary to ensure neither party causes prejudice to the unlawful activity of the other by releasing personal data disclosed by one party to the other, or indication 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.

10.2.2. 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.

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

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

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

10.2.6. Both parties will otherwise handle such requests in accordance with the DPA 2018 and GDPR.

10.3. Fair processing and privacy notices

10.3.1. 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.

10.3.2. ACRO will maintain a general notice, describing the mandatory privacy information at Articles 13 and 14 of GDPR and s44(1) and (2) DPA 2018. ACRO will not contact the data subjects directly with this privacy information on the basis that SFO-SC has already taken steps to inform the individual, or has exercised an appropriate exemption to article 13 or 14, or exercised an exemption at s44(4) DPA 2018.

10.3.3. SFO-SC 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 SFO-SC does not provide this information to the data subject, ACRO agrees to rely upon the correct use of an exemption by SFO-SC and will not contact the data subject to avoid the same prejudice.

11. Reuse of Personal Data Disclosed under this Agreement

11.1. 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 party that provided the information in the first instance, unless required to by law.

12. Roles and Responsibilities

12.1. Disputes

12.1.1. ACRO and the SFO-SC will designate Single Points of Contact (SPOC) who will work together to jointly solve problems relating to the sharing of information under this Agreement and act as point of contact in the event of a suspected breach by either party.

- ACRO (UK PNC enquiries and updates):
  ACRO Head of Section
  ****
- ACRO (International requests):
  ACRO Head of Section
  ****
- SFO (SC):
  Deputy Departmental Security Officer: ****
  ****
- SFO (SC):
  Departmental Security Officer: ****
  ****

12.1.2. Initial contact should be made by email with the subject heading:
FAO ACRO/SFO-SC ISA SPOC Ref no: XXXX

12.1.3. 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.

12.2. Escalation

12.2.1. 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: (Information Management)
  Records Management Supervisor
  ****
- SFO (SC):
  Departmental Security Officer: ****
  ****

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

13. Charges

13.1. Price and Rates

13.1.1. The SFO-SC shall pay ACRO for the provision of services set out in this Agreement and in line with the "Letter of Charges" provided to SFO-SC separately and are reviewed annually.

14. Review

14.1. Frequency

14.1.1. This ISA will be reviewed six months after implementation and annually thereafter.

15. Signature

15.1. Undertaking

15.1.1. 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.

15.1.2. Signatories must ensure compliance will all relevant legislation.

Signed on behalf of ACRO	Signed on behalf of SFO-SC
Position Held: Head of ACRO	Position Held: Security Advisor
Date: 24/07/2019	Date: 09/07/2019