ACRO
Criminal Records Office

Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

Insolvency Service (IS)

NPCC National Police Chiefs' Council
ACRO Criminal Records Office

The Insolvency Service

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 Insolvency Service (IS).
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 Insolvency Service (IS) 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 IS for recordable and non-recordable offences. In addition, this Agreement allows for the recording of details on to the PNC of individuals prosecuted in accordance with the Criminal Justice Act 2003 where the IS act as the Prosecuting Agent. The relevant offences are those committed in connection with fraud, personal and corporate insolvency and corporate misconduct.
Author	Information Management Development Officer
Renewal Date	12/08/2021
Date Issued	12/08/2020
ISA Ref	ACRO/015
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 001

Contents

Version Record

Version No.	Date	Amendments Made	Authorisation
1.0	15/07/2020	*Annual renewal, time and date amendments according to year of agreement and processing requirements.*	*KN, ACRO*

1. Partners to the Agreement

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

1.2. Insolvency Service (IS)
Criminal Enforcement
1 Victoria Street
London
SW1H 0ET

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.

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 S11 (2)).

Data Protection Legislation: the General Data Protection Regulation as enacted into English law (**GDPR**) as revised and superseded from time to time; the Data Protection Act 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.

NPA: Non Police Agency

NPPA: Non Police Prosecuting Agency

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 (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.

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

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 shall be prohibited (GDPR 2018 Article 9)

Subject Information Rights: means the exercise by a data subject of his or her rights under Articles 13-22 of the GDPR.

Supervisory Authority: the Information Commissioner or country equivalent.

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.

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

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

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

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.

A reference to **writing** or **written** includes email.

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. Purpose

3.2. 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 Insolvency Service (IS) 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 IS for recordable (and non-recordable offences where they are recorded on PNC).

3.2.1. This Agreement also formalises the arrangements for ACRO to record details and offences on to the PNC of individuals prosecuted in accordance with the Criminal Justice Act 2003 where the IS act as the Prosecuting Agent. The relevant offences are those committed in connection with fraud, personal and corporate insolvency and corporate misconduct.

3.2.2. 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

3.3. Background

3.3.1. 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.

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

3.3.3. IS are an executive agency of the Department for Business, Energy and Industrial Strategy. IS are a government agency that helps to deliver economic confidence by supporting those in financial distress, tackling financial wrongdoing and maximising returns to creditors.

4. Powers

4.1. IS Legal Basis

4.1.1. The IS is a competent authority as an Executive Agency of the Department for Business Energy and Industrial Strategy (BEIS), established under Section 30(1)(a) and Schedule 7 para 1 of DPA 2018. The IS undertakes the 'law enforcement' functions of the Secretary of State for BEIS, a 'relevant prosecutor' with the general statutory power to institute criminal proceedings under the Criminal Justice Act 2003 – Section 29(5)(e) and SI 2011 No. 2188 para 3(b).

4.1.2. The Secretary of State also has specific statutory powers to institute/consent to criminal proceedings including the following:

- Offences within Chapter VI of Part IX of the Insolvency Act 1986 'Bankruptcy' and under the Insolvency (England and Wales) Rules 2016 SI 2016 No. 1024 – Section 350(5) IA 1986
- Sections 448 to 451 and 453A Companies Act 1985; Sections 458, 460, 798, 949, 953, 1112 and paras 5 and 6 of sch. 1B of the Companies Act 2006 – Section 1126 CA 2006

4.1.3. It is a competent authority for the purposes of law enforcement processing to the extent of these powers.

4.1.4. 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.

4.1.5. The IS investigations and prosecutions activities are concerned with the following offences:

- Fraud Offences under the Fraud Act 2006
- Offences in connection with personal and corporate insolvency and restrictions on the use of company names under the Insolvency Act 1986
- Offences under the Company Directors Disqualification Act 1986
- Offences in respect of corporate misconduct under the Companies Acts 2006 and 1985 including Fraudulent Trading (Section 993, CA 2003)
- Offences of Theft, False Accounting and Forgery under the Theft Act 1968 and Forgery and Counterfeiting Act 1981
- Offences against public justice under Perjury act 1911 and common law (Perverting the Course of Justice)
- Inchoate and statutory conspiracy offences in respect of the above and common law Conspiracy to Defraud.
- Offences under section 798, paragraphs 5 and 6 of Schedule 1B to the Companies Act 2006

4.1.6. The IS 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

- Legal claims
- Anti-fraud organisations
- Archiving, Statistics, Research

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 and non-police prosecuting agencies.

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 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.

4.4. Human Rights Act 1998

4.4.1. 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.

4.4.2. 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.

4.5. Common Law Duty of Confidentiality

4.5.1. 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.

5. Process

5.1. Overview

5.1.1. ACRO, in response to requests made by the IS, will conduct PNC searches and provide a PNC print to meet the information needs ofIS. ACRO will also create an Arrest Summons Number (ASN) on the PNC in relation to the Impending Prosecution.

5.1.2. 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, 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

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

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

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

5.2 PNC Searches

5.1.1 Requests for a PNC search are to be made by the IS on a 'Names Enquiry' form which will be supplied by ACRO separately.

5.1.2 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
- IS 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 IS. This response will also indicate that in the absence of fingerprints the identity of the subject cannot be verified. Similar wording will apply to 'Trace' returns i.e. when a record is found and a PNC print provided.

5.2 Additional Information Requirements

5.2.1 Other personal data which the IS 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.

5.2.2 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 IS normal administrative procedures.

5.2.3 If required, ACRO will seek additional information from the IS to verify the identity of the subject of the request via the following secure IS mailbox:
****

5.2.4 No other mailbox is to be used unless this Agreement is updated to reflect a change of 'nominated' point of contact for the IS.

5.2.5 All email communication containing personal and conviction data will be exchanged using password protected ***** files if a secure email is not available.

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

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

5.4 Contingency Backup

5.4.1 In an event where IS require ACRO to provide a contingency service for PNC requirements, a discussion would be needed, prior to any checks, in order to establish volumes and expected turnaround times. This is necessary in order to ensure ACRO can cope with the demand.

6 Submission

6.1 Names Enquiry Forms

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

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

6.2 Telephone Requests

6.2.1 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 IS staff; **********

7 Provision of Information

7.1 Response to a PNC 'Names' Search

7.1.1 In response to a formal application, written or verbal, ACRO will provide the IS 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 IS. The content of each type of print is defined in the list of PNC Printer Transactions which will be supplied by ACRO separately.

7.1.3 If the IS 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:

****

7.1.4 The IS 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.

8 Recording Convictions on the PNC

8.1 Creating Records on the PNC

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

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

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

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

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

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

8.1.7 If, once a PNC record has been created by ACRO and an ASN issued to the IS, a decision is taken to deal with the offender by way of an 'Out of Court disposal' or proceedings are otherwise concluded by way of a discontinuance or 'No Further Action (NFA)' disposal, for instance on the advice of the Crown Prosecution Service (CPS), the IS 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 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 exception to consult should reuse 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) Informaiton Secuirty 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.

9.2.3 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.

9.3 Volumes

9.3.1 Is it estimated that for the year 2020-21, the IS will request c100 PNC checks and c150 PNC records to be created.

9.3.2 The IS will advise ACRO if the number of PNC checks 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 IS should only be made over a secure communication network and care must be taken where personal information is shared or discussed.

9.4.2 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.

9.4.3 The IS reference number must be included in the subject field of every email sent to ACRO.

9.4.4 Where email transmission is unavailable, records may be transferred by post via encrypted disk, 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 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 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 IS or a third party, the IS 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 on all cases submitted to ACRO except where ACRO requires further information from the IS to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by the IS.

10.3.2 Responses to requests for additional information must be made by the IS within 10 working days. 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 parties' control, this will be informed to the other party as soon as practical.

10.3.4 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.

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

10.3.6 ACRO will complete/update a record on the PNC within 3-5 *(usually three)* working days of the receipt of a completed NPA form from the IS 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 the IS including:

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

11 Complaints and Breaches

11.1 Complaints

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

11.2 Breaches

14.2.1. 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 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).

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

14.2.3. 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.

14.2.4. 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.

14.2.5. All security incidents and breaches involving police data shared under this agreement must be reported immediately to the 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 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 ciompliance 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 Freedom of Information Act 2000 in respect of information provided by or relating to the information provided by ACRO, the IS 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

12.1.4 The decision as to whether to disclose the information remains with IS, 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 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.

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 the IS receives a relevant request, the IS representative is contact the NPCC Data Protection Officer at: data.protection@npcc.pnn.police.uk to ascertain whether the NPCC wishes to propose to the IS that they apply any relevant exemptions when responding to the applicant.

12.2.5 Where ACRO receives a relevant request, the NPCC Data Protection Officer is to contact the IS representatives to ascertain whether the IS 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 DPA 2018 and GDPR.

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 GDPR and s44(1) and (2) DPA 2018. ACRO will not contact the data subjects directly with this privacy information on the basis that IS 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.

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

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

14 Roles and Responsibilities

14.1 Disputes

14.1.1 ACRO and the IS 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
  ****
- IS:
  Deputy Head of Paralegal: **********
  ****
- IS:
  Management Team : **********
  ****

14.1.2 Initial contact should be made by email with the subject heading:
FAO ACRO/IS 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:
  ACRO Information Management Team: Records Management Supervisor
  ****
- IS:
  Deputy Head of Paralegal: **********
  ****

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

15 Charges

15.1 Price and Rates

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

15.2 Invoices

15.2.1 Invoices shall contain the following information:

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

15.2.2 The Purchase Order Number is to be provided by the IS 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 IS 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 IS.

15.2.4 If the IS 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 six months after implementation and annually thereafter.

16.1.2 This Information Sharing Agreement is an annual renewal for the year 2020/21.

17 Signature

17.1 Undertaking

17.1.1 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.

17.1.2 Signatories must ensure compliance will all relevant legislation.

Signed on behalf of ACRO	Signed on behalf of IS
Signature: **********	Signature: **********
Full Name: Robert Price	Full Name: **********
Position Held: Chief Executive	Position Held: Deputy Head of Paralegal
Date: 13 August 2020	Date: 12 August 2020