Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

Home Office Customer Services Group

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 Home Office (HO) Customer Services Group (CSG).
Version	2.0
Summary	This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for ACRO, acting on behalf of UK police forces that are subject to the section 22A Collaboration Agreement, to provide CSG with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands, information markers and final warnings for the assessment of visa applications to enter the UK. This service involves checking and the provision of PNC records when a 'hit' is made on IDENT1, in relation to fingerprints obtained as part of the visa application process.
Author	****, Information Governance Officer
Date Issued	19/09/2024
Review date	21/06/2025
Expiry date	19/09/2025
ISA Reference	ACRO/044
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 044

Contents

Version control

Version No.	Date	Amendments Made	Authorisation
0.1	23/07/2020	Annual Renewal	KN, ACRO
0.2	31/12/2020	Post-new services exploration updates for annual renewal	KN, ACRO
0.3	28/05/2021	DPO renewal updates	KN, ACRO
0.4	09/07/2021	UKVI Certificate Process updates	KN, ACRO
0.5	12/08/2021	HO UKVI updates	JK, HO
1.0	28/09/2021	Signed Agency Version	AM, ACRO
1.1	14/03/2023	2023/24 Annual Renewal.	MH, ACRO
1.2	31/01/2024	DPO review	AAS, ACRO
1.3	06/02/2024	Addition to Powers section	MH, ACRO
1.4	09/02/2024	DPO review following updates from agency	AAS, ACRO
1.5	14/03/2024	PNCS Process review/ amendments	PNC SCRAs/EC, ACRO
1.6	21/05/2024	Directorate name updates to CSG	MH, ACRO
1.7	02/07/2024	DPO Review	AAS, ACRO
1.8	30/07/2024	HO CSG sign off and Logo update	HO CSG
1.9	07/08/2024	ACRO SIRO Signature	JF, ACRO
2.0	24/09/2024	NPCC Signature	NPCC

1. Parties to the Agreement

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

1.2. Customer Services Group, Home Office
Lunar House
40 Wellesley Road
Croydon
CR9 2BY

2. Agreed Terms

2.1. Interpretation

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

2.1.1. Definitions:

ACRO: ACRO Criminal Records Office.

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

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

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

CEO: Chief Executive Officer

CRO: Criminal Record Office Number, a unique identifier allocated to an individual the first time they are charged with a recordable offence.

CSG: Customer Service Group, Home Office

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

Eurodac: Immigration Fingerprint Database, contains the fingerprints of anyone who has made an asylum or immigration application, anywhere in Europe.

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

FTA: Failure to Appear (to Court).

GSCP: Government Security Classification Policy.

HIOWC: Hampshire & Isle of Wight Constabulary

HO: Home Office

IDENT1: National automated fingerprint database that provides biometric services to Forces and Law Enforcement Agencies.

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

OI Marker: Operational Information Marker

OIC: Officer in charge (of a case)

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

PACE: Police and Criminal Evidence Act 1984

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, this will be migrating to the Law Enforcement Data Service (LEDS) therefore the reference to PNC will cover both PNC/LEDS whichever system is in place at the time.

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.

Tenprint: International Association for Identification's Certification Program, which uses certified examiners to practice fingerprint friction ridge identification and comparison.

The Agency: Where this document refers to The Agency, this is interpreted as the Non-Police Agency who sign to the services under this Agreement, as detailed at section 1.2. of this Agreement.

UK: United Kingdom

UKEC: United Kingdom Entry Clearance (certificate)

UKVI: United Kingdom Visas and Immigration

WinZip: trialware file archiver and compressor for Microsoft Windows

WM: Wanted/Missing Marker

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 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 Agencies (NPAs) and assists safeguarding processes conducted by relevant agencies.

3.1.2. CSG are a HO Directorate that brings together colleagues within 7 cross-cutting functions of Customer Services. Following some structural changes in the HO in 2023/24, processing formerly conducted under the UK Visas and Immigration (UKVI) directorate, such as the statutory function to manage immigration by the consideration and processing of Visa applications and management of the UK asylum service, is now carried out by CSG.

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, acting on behalf of UK police forces that are subject to the s22A Collaboration Agreement, to provide CSG with access to relevant information held on the Police National Computer (PNC), specifically convictions, cautions, reprimands, final warnings, and information markers. It is necessary for CSG to have access to such information to assist the Home Office with their statutory duty for the assessment of visa applications, made to enter the UK. The nature of the information required by CSG includes both recordable and non-recordable offences.

3.2.3. The aim of the data sharing initiative is to provide a bespoke PNC Disclosure, by way of an ACRO UK Entry Clearance (UKEC) certificate, as required by CSG for recordable and non-recordable offences. It will serve to benefit society by enabling them to fulfil their statutory duty and conduct a holistic review of visa applications to support public protection.

3.2.4. 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.

3.2.5. The parties agree to only process Shared Personal Data, (i) in the case of the CSG 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. Home Office Customer Service Group Legal Basis

4.1.1. CSG require data collected for a law enforcement purpose for the general purpose of assessing visa applications. This processing is authorised by law under the Immigration and Asylum Act 1999, section 20 Power to supply information etc., to Secretary of State, and the Immigration Act 1971 section 3(6), which outlines the grounds for which leave to enter by application of a Visa may be declined. For example, where a non-British Citizen has been convicted of an offence punishable with imprisonment. The UK Borders Act 2007, section 43, outlines the requirement for conviction data to assist with the decision-making process essential for the assessments of Visas.

4.1.2. The Secretary of State, under powers outlined at section 3(2) of the Immigration Act 1971, provides, and can change the regulatory rules, known as Immigration Rules, required of an individual to enter the UK. The Immigration Rules provide guidelines to CSG caseworkers on the requirements, such as Part 9: Grounds for Refusal, regarding the use of spent and/or unspent convictions as evidence in their assessments.

4.1.3. The processing of these data meets a condition of Article 6(1) of UK GDPR. Conditions under Article 6(1)(e) are further described at section 8 of the Data Protection Act (DPA) 2018. The conditions met are:

- Performance of a public task in the public interest or official authority.

4.1.4. The processing of these data meets an exemption under Article 9(2) of UK GDPR relating to the processing of special categories of personal data. The exemptions met are:

- Substantial Public Interest.

4.1.5. The processing of these data meets a condition under Schedule 1 of the DPA 2018, as per section 10 of the same Act, relating to the processing of special categories of personal data and criminal conviction or offence data. The conditions met are:

- Statutory etc. and Government purposes.

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 Hampshire & Isle of Wight Constabulary (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, that are Joint Controllers under the Joint Controllers Agreement, to provide PNC enquiry, update and disclosure services to Non-Police Agencies (NPAs) and Non-Police Prosecuting Agencies (NPPAs).

4.2.3. ACRO is a Competent Authority, by virtue of the section 22A Agreement, processing data for a law enforcement purpose.

4.2.4. Under the first Data Protection Principle, processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law. Under section 35(2) of the DPA 2018 the following applies:

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

4.2.5. Under section 35 (3) to (5) and Schedule 8 of the DPA 2018, ACRO meets the conditions for sensitive processing as follows:

- Administration of justice.

4.3. Code of Practice for the Management of Police Information

4.3.1. This Agreement outlines the need for the Police and Partners to work together to share information in line with the Policing Purposes as set out in the Management of Police Information Code of Practice. In line with section 39A of the Police Act 1996, Chief Officers are required to give "due regard" to this statutory code. The Policing Purposes summarise the statutory and common law duties of the police service for which personal data may be processed and are described as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice; and
- Any duty or responsibility arising from common or statute law.

4.4. Human Rights Act 1998

4.4.1. Under Schedule 1, Article 8 of the Human Rights Act 1998, all data subjects have a right to respect for their private and family life, home and correspondence.

4.4.2. Interference with this right may be justified when lawful and necessary and in the interests of:

- Discharging the common law police duties;
- Preventing/detecting unlawful acts;
- Protecting the public against dishonesty, etc.;
- Preventing fraud;
- Terrorist finance/money laundering;
- Safeguarding children and adults at risk;
- Safeguarding the economic wellbeing of vulnerable adults.

4.5. Common Law Police Disclosure

4.5.1. Where legislation provides the organisation with a power to process Personal Data for a specific purpose, but there is no explicit legislative authority for requesting the disclosure of the data for the organisation's specified purpose, the disclosure may be carried out on the grounds of Common Law Police Disclosure, i.e. only where there is a pressing social need. 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);
- 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 Threat Check Team in CSG, will conduct a PNC search and upon a match on IDENT1, will produce a bespoke ACRO UKEC disclosure certificate, designed to meet Visa decision-making requirements.

5.1.2. The Certificate will comprise of the following identification data:

a) Personal data (if available): name, date of birth, birth place, sex, all recorded addresses, aliases (including DVLA name) and alias date of births.

b) Recorded address will not include those for business, friend, parents/relatives, prisons, language schools, foreign addresses outside UK, blanks and additional.

5.1.3. The Certificate will comprise of the following PNC data (if available):

a) Convictions, non-convictions, and impending convictions,

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

5.2. PNC Searches via IDENT1

5.2.1. Requests for a PNC search are automatically received through IDENT1.

5.2.2. The following Personal Data is to be provided by ACRO in support of each request (where known) as a minimum:

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

5.2.3. CSG in support of a PNC search will also provide the following information (where known):

- Recording event
- Case type
- Result (of IDENT1 check)
- Eurodac
- Biometric Received date.
- Decision location

- IDENT1 name
- CRO

5.2.4. Where a Names Enquiry search is conducted and a match is made on PNC, ACRO PNC Services will produce an ACRO UKEC Certificate.

5.2.5. If a CRO number returns a 'No Trace' result on PNC, ACRO will verify the reference and purpose with Tenprint. Should the fingerprints be recorded for identification purposes only, a pseudo-set, ACRO will notify CSG that the CRO does not relate to any criminal data.

5.2.6. In the event that the PNC record exists but the CRO has been weeded under the Protection of Freedoms Act (PoFA), ACRO will produce an ACRO UKEC Certificate containing the following wording; "The CRO number is currently showing as being deleted due to fingerprint destruction under the Protection of Freedoms Act. So, whilst the PNC record is still in existence there are no accompanying fingerprints. Identity cannot be confirmed without the existence of fingerprints, and we have created this certificate without the use of a CRO number."

5.2.7. All responses will be returned to CSG, password protected, in Adobe.

5.3. Intel Certificate

5.3.1. Where a record comes to notice following a CSG request, which contains relevant information markers, an Intel certificate may be produced to accompany the ACRO UKEC certificate and support the Agency in the assessment of the Visa application. The Intel certificate is only provided if the agreed, relevant markers are present on a Subject's PNC record.

5.4. Additional Information Requirements

5.4.1. Other personal data, which the CSG 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.

5.4.2. 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 CSG normal administrative procedures.

5.4.3. If required, ACRO will seek additional information from CSG to verify the identity of the subject of the request via the following CSG mailbox: ****@homeoffice.gov.uk

5.4.4. All e-mail communication containing personal and conviction data will be exchanged using password protected files and sent via secure e-mail.

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

5.4.6. Where appropriate, CSG 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 CSG require ACRO to provide a contingency service for PNC requirements in line with the Agreed Services, discussion must be had, prior to any checks, in order to establish volumes and expected turnaround times. This is necessary in order to ensure ACRO can provide the required service and cope with the demand.

6. Submission

6.1. Police Search Results

6.1.1. CSG will contact IDENT1 in the first instance. ACRO will receive any matches made by IDENT1 on a Police Search Result form, via automated secure e-mail to the following e-mail address: ****@acro.police.uk

6.1.2. Erroneous or incomplete IDENT1 results will not be processed. They will be returned to CSG as invalid and a reason provided.

6.2. Telephone Requests

6.2.1. Requests may be made by telephone in cases of emergency. A Police Search Result form must be submitted in advance, with a call to expedite an existing check then 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 CSG staff. As at the date of this Agreement, the CSG staff who will have the ability to make telephone requests shall be ****, Higher Executive Officer (HEO); **** Senior Executive Officer (SEO); **** Assistant Director (G7); ****, Executive Officer (EO), ****, Executive Officer (EO).

6.2.3. CSG may update this list by notice to ACRO from time to time.

7. Provision of Information

7.1. Response to a IDENT1 Police Search Result/PNC Names Enquiry Search

7.1.1. In response to a formal written application, ACRO will provide a UKEC certificate to CSG with the following information derived from the PNC in response to applications made in accordance with this Agreement:

- All convictions, non-convictions, and impending convictions.
- 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. Where a record comes to notice containing additional information markers that may assist CSG in the assessment of a Visa application, an accompanying Intel certificate may be produced.

7.1.3. It should be noted that the service provided under this Agreement only covers the provision of an ACRO UKEC Certificate, and an Intel Certificate where applicable, depending on the request submitted by CSG.

7.1.4. If CSG 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

7.1.5. CSG will need to liaise directly with forces to obtain further detailed explanation 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. Information Security

8.1. Government Security Classification Policy

8.1.1. 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.

8.1.2. 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.

8.2. Security Standards

8.2.1. It is expected that parties 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. Parties are at liberty to request copies of each other's:

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

8.2.2. 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.

8.2.3. 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.

8.2.4. 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.

8.2.5. 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.

8.3. Volumes

8.3.1. It is estimated that for the year 2024/25, CSG will request up to 4,000 PNC Checks.

8.3.2. CSG will advise ACRO if the number of PNC checks is likely to be exceeded.

8.3.3. 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.

8.4. Transmission

8.4.1. With the exception of telephone requests in cases of emergency, contact between ACRO and CSG should only be made over a secure communication network by the email addresses agreed in this Agreement, and care must be taken where personal information is shared or discussed.

8.4.2. 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.

8.4.3. A CSG reference number must be included in the subject field of every e-mail sent to ACRO.

8.4.4. Where e-mail transmission is unavailable, records may be transferred by post via encrypted media only, where encryption meets current industry standards.

8.5. Retention and disposal

8.5.1. 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.

9. Information Management

9.1. Accuracy of Personal Data

9.1.1. 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 parties to this Agreement of the erasure or rectification.

9.1.2. 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.

9.1.3. 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.

9.2. Accuracy Disputes

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

9.3. Turnaround

9.3.1. This Agreement requires a seven (7) working day turnaround (not including day of receipt or response) on all requests submitted to ACRO for PNC data, except where ACRO requires further information from the CSG to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by CSG.

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

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

9.3.4. An exception to the seven (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.

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

9.4. Quality Assurance and Control

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

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

- Number of IDENT1 Police Searches received
- Number of PNC 'Names Enquiry' forms received
- Number of ACRO UKEC Certificates provided
- Details of any cases that fall outside agreed 'Service Levels'
- Number of issues and/or disputes

10. Complaints and Breaches

10.1. Complaints

10.1.1. 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.

10.2. Breaches

10.2.1. 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 sections 67 and 68 of the DPA 2018. Each party 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).

10.2.2. 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.

10.2.3. 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.

10.2.4. 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.

10.2.5. 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.

11. Information Rights

11.1. Freedom of Information Act 2000

11.1.1. 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.

11.1.2. 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.

11.1.3. 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 CSG 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

11.1.4. The decision as to whether to disclose the information remains with CSG but will be made with reference to any proposals made by the NPCC.

11.2. Data Subject Information Rights

11.2.1. 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.

11.2.2. 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.

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

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

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

11.2.6. Both parties will otherwise handle such requests in accordance with the Data Protection Legislation.

11.3. Fair processing and privacy notices

11.3.1. 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.

11.3.2. 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 CSG 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.

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

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

12.1. 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.

13. Roles and responsibilities

13.1. Single Point of Contact

13.1.1. ACRO and CSG 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
  ****

- Customer Services Group – Threat Check Team
  ****
  Operational Manager
  **** @homeoffice.gov.uk
  ****

13.1.2. Initial contact should be made by e-mail with the subject heading:
FAO ACRO/ HO CSG ISA SPOC Ref no: XXXX

13.1.3. 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.

13.2. Escalation

13.2.1. In the event that the nominated SPOC cannot agree on a course of action or either party appears not to have met the terms and conditions of this Agreement, the matter should initially be referred jointly to the following:

- ACRO (UK PNC enquiries and updates):
  ACRO National Services Deputy Manager
  **** @acro.police.uk
  ****

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

- Customer Services Group – Threat Check Team
  ****
  Assistant Director

**** @homeoffice.gov.uk
****

13.2.2. Both ACRO and CSG 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.

14. Charges

14.1. Price and Rates

14.1.1. CSG shall pay ACRO for the provision of services set out in this Agreement and in line with the "Letter of Charges" provided to them separately, which is reviewed annually.

14.2. Invoices

14.2.1. 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 CSG).

14.2.2. The Purchase Order Number is to be provided by CSG 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.

14.2.3. CSG 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 CSG.

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

15. Review

15.1. Frequency

15.1.1. This ISA will be reviewed nine months after implementation and renewed annually thereafter.

15.1.2. This Agreement is for 2024/25.

16. Variation

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

17. Waiver

17.1. 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.

18. Severance

18.1. 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.

18.2. If any provision or part-provision of this Agreement is deemed deleted under clause 18.1, 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.

19. Changes to the applicable law

19.1. 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.

20. No partnership or agency

20.1. 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.

21. Notice

21.1. 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.

21.2. Notice of a cessation of services, or end to the requirement of services, will be given by either party with a period of 3 months' notice for a specified date of cessation.

21.3. ACRO reserves the right to give Notice of cessation with immediate affect where The Agency is found to no longer have a lawful basis for requesting conviction data, is under investigation for the misuse of conviction data, or found to be in other serious breach of the Terms of this Agreement.

21.4. 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.

21.4.1. 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.

21.5. 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.

22. Signature

22.1. Undertaking

22.1.1. 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.

22.1.2. Signatories must ensure compliance with all relevant legislation.

Signed on behalf of ACRO Senior Information Risk Owner (SIRO)	Signed on behalf of Customer Services Group
Full Name: ****	Full Name: ****
Position Held: CEO of ACRO	Position Held: Assistant Director
Date: 07/08/2024	Date: 30/07/2024

22.1.3. 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: DCC Operational Communications in Policing (OCiP)
Date: 19/09/2024