Information Sharing Agreement

Between

National Police Chiefs' Council
ACRO Criminal Records Office

And

Sky UK Limited.

Summary Sheet

Freedom of Information Act Publication Scheme	
Security Classification (GSC)	OFFICIAL
Publication Scheme Y/N	No
Title	Information Sharing Agreement between ACRO Criminal Records Office (ACRO) and Sky UK Limited (Sky).
Version	2.0
Summary	This Information Sharing Agreement (hereafter referred to as the Agreement) formalises the arrangements for ACRO to provide Sky with access to relevant information held on the Police National Computer (PNC), S.31(1) [redacted] Furthermore, this Agreement also allows for the recording of details of individuals prosecuted by Sky under the Prosecution of Offences Act 1985, Copyright Designs and Patents Act 1988, Proceeds of Crime Act 2002, Serious Crime Act 2007, Fraud Act 2006, Criminal Justice Act 1987, and other recordable offences where Sky act as the Non-Police Prosecuting Agent on to the PNC S.31(1) [redacted] S.31(1) [redacted]
Author	S.40(2) [redacted] Information Governance Officer S.40(2) [redacted] Information Governance Supervisor
Date Issued	28/10/2025
Review date	01/04/2026
Expiry date	27/10/2026
ISA Reference	ACRO/207
Location of Agreement	ACRO ISA Library
ACRO DPIA Reference	DPIA 207

Contents

Summary Sheet 2
Version control 5
1. Parties to the Agreement 6
2. Agreed Terms 7
2.1. Interpretation 7
3. Purpose and background of the Agreement 10
3.1. Background 10
3.2. Purpose 10
4. Powers 12
4.1. Sky UK Ltd Legal Basis 12
4.2. ACRO Legal Basis 13
4.3. Code of Practice for the Management of Police Information 14
4.4. Human Rights Act 1998 14
4.5. Common Law Police Disclosure 14
4.6. Crime and Disorder Act 1998 14
4.7. The Policing Protocol Order 2011 15
5. Process 15
5.1. Overview 15
5.2. PNC Searches 16
5.3. Additional Information Requirements 17
6. Submission 18
6.1. Names Enquiry Spreadsheets 18
6.2. Telephone Requests 18
7. Provision of Information 19
7.1. Response to a PNC Names Enquiry Search / Witness Search 19
8. Recording Convictions on the PNC 20
8.1. Creating Records on the PNC 20
9. International Requests 20
9.1. Process 20
9.2. Exchange of Criminal Records with the EU 21
9.3. Exchange of Criminal Records with Non-EU Countries 22
9.4. Specific Data Handling 22
10. Information Security 23
10.1. Government Security Classification Policy 23

10.2. Security Standards 23
10.3. Volumes 24
10.4. Transmission 24
10.5. Retention and disposal 24
11. Information Management 25
11.1. Accuracy of Personal Data 25
11.2. Accuracy Disputes 25
11.3. Turnaround 25
11.4. Quality Assurance and Control 26
12. Complaints and Breaches 26
12.1. Complaints 26
12.2. Breaches 26
13. Information Rights 27
13.1. Freedom of Information Act 2000 27
13.2. Data Subject Information Rights 28
13.3. Fair processing and privacy notices 28
14. Re-use of Personal Data Disclosed under this Agreement 29
15. Roles and responsibilities 29
15.1. Single Point of Contact 29
15.2. Escalation 30
16. Charges 31
16.1. Price and Rates 31
16.2. Invoices 31
17. Review 31
17.1. Frequency 31
18. Variation 32
19. Waiver 32
20. Severance 32
21. Changes to the applicable law 32
22. No partnership or agency 32
23. Notice 32
24. Signature 34
24.1. Undertaking 34

Version control

Version No.	Date	Amendments Made	Authorisation
0.1	21/11/2022	Original Draft	S.4 ACRO
0.2	24/02/2023	DPO Review	S. , ACRO
0.3	06/03/2023	Administrative Changes	S. , ACRO
0.4	27/04/2023	Administrative Changes	S.4 ACRO
0.5	18/09/2023	Changes by Sky UK	S. , ACRO
0.6	20/09/2023	Removed applicable sections	S.4 ACRO
0.7	20/03/2024	Signed by Sky UK	S. , ACRO
0.8	21/03/2024	Signed by S	S.4 ACRO
1.0	07/05/2024	Signed by NPCC Lead	S.4 ACRO
1.1	08/08/2025	Draft renewal	S.40 ACRO
1.2	18/08/2025	IGS Review	S.4 ACRO
1.3	21/08/2025	DPO review	S.40 ACRO
1.4	15/10/2025	Changes by Sky UK	S.4 ACRO
1.5	22/10/2025	Signed by Sky UK	Sky UK
1.6	22/10/2025	Signed by ACRO SIRO	S. ACRO

1. Parties to the Agreement

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

Sky UK Limited ("**Sky**")
Grant Way,
Isleworth,
Middlesex.
TW7 5QD
ICO Registration Number (Z6165064)

2. Agreed Terms

2.1. **Interpretation**

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

2.1.1. Definitions:

ACRO: ACRO Criminal Records Office.

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

ASN: Arrest Summons Number.

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

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

CEO: Chief Executive Officer.

CPIA: Criminal Procedure and Investigation Act 1996

CPS: Crown Prosecution Service.

Criminal Offence Data is personal data relating to criminal convictions and offences or related security measures and includes personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing. (DPA 2018, section 11(2)).

Data Protection Legislation: the General Data Protection Regulation as enacted into English law (**UK GDPR**) as revised and superseded from time to time; the Data Protection Act 2018 (**DPA 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.

EEA: European Economic Area.

EIR: Environmental Information Regulations 2004.

EU: European Union.

FOI: Freedom of Information

FOIA: Freedom of Information Act 2000.

Great Britain: geographic term referring to the island consisting of England, Scotland and Wales.

GSCP: Government Security Classification Policy.

HIOWC: Hampshire & Isle of Wight Constabulary.

LEDS: Law Enforcement Data Service; national cloud-based data service for policing set to fully replace the Police National Computer (PNC) from March 2026. This will provide police forces and other law enforcement agencies with on-demand and joined-up information at their point of need. LEDS may be used prior to March 2026 dependent upon ACRO being on boarded as a user.

MB: Megabyte (of data).

NFA: No Further Action.

NPA: Non-Police Agency.

NPCC: National Police Chiefs' Council.

NPCC LEDS: National Police Chiefs' Council Law Enforcement Data Service; team involved in the delivery of the new LEDS national policing system.

NPPA: Non-Police Prosecuting Agency.

OIC: Officer in charge of the case.

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

PACE: Police and Criminal Evidence Act 1984

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. The data held on this national policing system will be migrating to the Law Enforcement Data Service (LEDS) with a planned decommission date of March 2026. Any reference to "PNC/LEDS" in this Agreement will be taken to cover both of these systems, whichever is in use at any given time.

ROA: Rehabilitation of Offenders Act 1974.

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.

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

Third Country: means a country or territory outside the United Kingdom (UK GDPR, Article 4 and DPA 2018, section 33(7)).

UK: United Kingdom; means Great Britain and Northern Ireland (Interpretation Act 1978, Schedule 1).

UKCA-ECR: UK Central Authority for the Exchange of Criminal Records.

WinZip: trialware file archiver and compressor for Microsoft Windows.

WM: Wanted Missing report.

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 hosted by Hampshire & Isle of Wight Constabulary (HIOWC) 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 United Kingdom (UK) and other countries. ACRO provides access to information held on the PNC to support the criminal justice work of some Non-Police Prosecuting Agencies (NPPAs) and assists safeguarding processes conducted by relevant agencies.

3.1.2. S.31(1) [redacted]

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 ACRO section 22A Collaboration Agreement, to provide Sky with access to relevant information held on PNC, S.31(1) [redacted]

3.2.3. Under this Agreement, Sky can request criminal conviction information held outside of the UK via ACRO when there is a lawful basis to do so.

3.2.4. Under this Agreement, Sky can request that ACRO create records on PNC for the purpose of prosecuting individuals under the Prosecution of Offences Act 1985, Copyright Designs and Patents Act 1988, Proceeds of Crime Act 2002, Serious Crime Act 2007, Fraud Act 2006, Criminal Justice Act 1987 and other recordable offences where Sky act as the NPPA. These will be updated on to the PNC for the purposes of investigations into offences committed in connection with digital piracy.

3.2.5. The aim of the data sharing initiative is to share relevant information pertaining to outstanding criminal offences committed in the England and Wales and other jurisdictions relevant and required by Sky for recordable and non-recordable offences. It will serve to benefit society by disrupting organised crime groups and tackling copyright crime and ensuring consumers continue to benefit from TV programmes, movies and music both now and in the future.

3.2.6. 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.

3.2.7. The parties agree to only process Shared Personal Data, (i) in the case of Sky, for the purposes outlined at 3.2.4 and 3.2.5., and (ii) in the case of ACRO, for the 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. Sky Legal Basis

4.1.1. S.31(1) [redacted] This processing is authorised by law under:

- Prosecution of Offences Act 1985 - s.6 (1) instituting any criminal proceedings
- Copyright Designs and Patents Act 1988 – s.107 Criminal liability for making or dealing with infringing articles
- Proceeds of Crime Act 2002 – s.327 Intentionally encouraging or assisting an offence
- Serious Crime Act 2007 – s.44 Intentionally encouraging or assisting an offence. S.45 Intentionally encouraging or assisting an offence
- Fraud Act 2006 – s.11 Obtaining services dishonestly
- Criminal Justice Act 1987 – charges and penalty for conspiracy to defraud

4.1.2. S.31(1) [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

4.1.3. Sky can request PNC data from ACRO to assist the assessment of prosecution witness suitability by use of the Witness Print. The Criminal Procedure and Investigations Act 1996 (CPIA), sections 3 and 7A, CPIA S.23(1) Code of Practice 5.4- 5.5, 6 and 7.4-7.6 and 8, and Attorney General's Guideline 2024, paragraphs 62, 80 and 86 outline Sky's responsibility as a prosecutor to ensure material will not undermine the prosecution.

4.1.4. The processing of this data has a lawful basis as per Article 6(1) of UK GDPR. Tasks that are carried out in the public interest under Article 6(1)(e) are further described under section 8 of the Data Protection Act (DPA) 2018. The lawful basis for this processing is:

- Legitimate interests test.

4.1.5. The processing of this data meets an exemption condition under Article 9(2) of UK GDPR and section 10 of the DPA 2018, regarding the processing of special categories of personal data. The exemption met is:

- Legal claims, judicial acts (courts, tribunal) and/or
- Substantial public interest.

4.1.6. The processing of this 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 convictions. The conditions met are:

- Preventing/detecting unlawful acts; and/or
- Preventing fraud (anti-fraud organisations).

4.2. **ACRO Legal Basis**

4.2.1. Section 22A of the Police Act 1996 enables police forces to discharge functions of officers and staff where it is in the interests of efficiency or effectiveness of their own and other police force areas. Schedule 7, Paragraph 17 of the DPA 2018 establishes bodies created under section 22A of the Police Act 1996 as Competent Authorities.

4.2.2. ACRO, hosted by HIOWC, is established through the National Police Collaboration Agreement relating to ACRO under section 22A of the Police Act 1996. This Agreement gives ACRO the authority to act on behalf of the Chief Constables who are Joint Controllers of PNC to provide PNC enquiry, update and disclosure services to Non-Police Agencies (NPAs) and NPPAs.

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

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

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

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

- Administration of justice.

4.2.6. ACRO have been delegated responsibility for managing the UK Central Authority for the Exchange of Criminal Records (UKCA-ECR). As such, ACRO discharge the UK's responsibilities under the 1959 Convention on Mutual Assistance in Criminal Matters and the Trade and Co-operation Agreement between the European Union and the United Kingdom, Part 3, Title IX on the exchange of information extracted from the criminal record.

4.2.7. ACRO also exchange conviction information with countries outside of the EU via Interpol channels, subject to Interpol Protocols.

4.3. **Code of Practice for the Management of Police Information**

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

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

4.4. **Human Rights Act 1998**

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

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

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

4.5. **Common Law Police Disclosure**

4.5.1. Common Law Police Disclosure (CLPD) is a legal principle that allows the police to share information with an employer or regulatory body when there is a pressing social need to protect public safety. This applies when no specific legislative authority exists for the disclosure of Personal Data, but there is a clear risk to public protection. In such cases, the police may disclose information to enable the employer or regulatory body to act quickly and reduce potential harm, provided the disclosure if necessary to address the pressing social need.

4.6. **Crime and Disorder Act 1998**

4.6.1. Under section 17 of this Act, the relevant authority has a legal duty to consider the impact of crime and disorder in its area and to take all reasonable steps to prevent the following:

- Crime and disorder in its area, including anti-social behaviour and any other actions that negatively affect the local environment;
- The misuse of drugs, alcohol and other substances in its area; and
- Reoffending within its area, aiming to reduce the likelihood of individuals reoffending.

4.6.2 The "relevant authority" refers to any local authority or organisation with responsibility for public safety, crime prevention, or the enforcement of law and order in a given area. This includes, but is not limited to, local councils, police forces, and other public bodies that work to address crime and social issues within their jurisdiction.

4.6.3 Under section 115(1), any individual or organisation that would not normally have power to disclose information to a relevant authority, or to a person acting on behalf of such an authority, is granted the power to disclose information when it is deemed necessary or expedient for fulfilling any purpose outlined within the Act. This provision allows for the sharing of information to support crime prevention, public safety and the effective enforcement of the law.

4.7. **The Policing Protocol Order 2011**

4.7.1 The Chief Constable is responsible for maintaining public order and upholding the King's Peace. They are legally accountable for the exercise of police powers and are also accountable to the Police and Crime Commissioner (PCC) for ensuring the efficient and effective delivery of policing services, as well as the management of resources and expenditure within the police force.

5. Process

5.1. **Overview**

5.1.1. ACRO, in response to requests made by Sky, will create an Arrest Summons Number (ASN) on the PNC in relation to the impending prosecution, will conduct PNC searches and provide a PNC print to meet their information needs. As a POA agency, Sky will only be provided a Prosecutor/Court multi-print once an ASN request has been made.

5.1.2. The PNC data will comprise of:

a) A 'Disclosure PNC Print' will include the following information:
   - Personal data (if available): name, date of birth, birthplace, sex, address, occupation, aliases (including Driver and Vehicle Licensing Agency (DVLA) name) and alias dates of birth. The home address that is printed in the ID part of the print is decided by the following rules:
     - If there is more than one home address on the record, the most recent address is used;

- If there is no home address present, the most recent 'no fixed abode' address type will be used;
- If neither of the above address types are present, the most recent 'Other' address is printed.

- Criminal Offence Data (if any such data exists): convictions, cautions, warnings, reprimands and impending prosecutions.
- Special categories or personal data: it may be possible to discern political opinions, religious or philosophical beliefs or sexual orientation from the nature of an individual's offending

b) A Prosecutor's and Court Multiple print. The personal data disclosed under this print includes (if available): name, date of birth, birth place, address, driver number, aliases (including DVLA name) and alias dates of birth. The home address that is printed in the ID part of the print is decided by the following rules:
   - If there is more than one home address on the record, the most recent address is used;
   - If there is no home address present, the most recent 'no fixed abode' address type will be used;
   - If neither of the above address types are present, the most recent 'Other' address is printed.

c) A Witness PNC print. The personal data disclosed under this print includes (if available): name and alias names.

5.1.3. If relevant, ACRO shall provide to Sky for onward provision to the court a PNC Prosecutor's and Court Multiple 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 Sky 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 Agency.

5.2. **PNC Searches**

5.2.1. Requests for a PNC search are to be made by Sky on a 'Names Enquiry' spreadsheet which will be supplied by ACRO separately.

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

- First name;

- Any middle names;
- Surname/family name;
- Date of birth (dd/mm/yyyy);
- Any alias details (names, dates of birth etc.);
- Place of birth (where known);
- Address;
- The Sky 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 Agency. In the absence of fingerprints the identity of the subject cannot be verified. Similar wording will apply to 'Trace' returns i.e. when a record is found and a PNC print provided.

5.3. **Additional Information Requirements**

5.3.1. Other personal data, which Sky caseworker may be aware of e.g. National Insurance Number, Passport or Driving Licence Number etc. can be provided to aid identification. This additional information will be used to confirm identity and is of particular value where the name or other personal details are identical on the PNC.

5.3.2. It is not necessary to obtain the additional information as a matter of course particularly if it is not currently recorded as part of Sky normal administrative procedures.

5.3.3. If required, ACRO will seek additional information from Sky to verify the identity of the subject of the request via the following Sky mailbox: S.31(1)

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

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

6. Submission

6.1. Names Enquiry Spreadsheets

6.1.1. Completed 'Names Enquiry' spreadsheets are to be sent via secure e-mail to the following e-mail address: S.31(1) [redacted]

6.1.2. ACRO will receive requests from The Agency, via the following secure mailbox: S.31(1) [redacted]

6.1.3. Erroneous or incomplete 'Names Enquiry' spreadsheets will not be processed. They will be returned to Sky as invalid and a reason provided.

6.2. Telephone Requests

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

6.2.2. Whilst ACRO may be able to assist expediting the processing of a Request Out to relevant foreign countries, there is still no guarantee that those countries will likewise respond quicker than they ordinarily would have done.

6.2.3. Such requests can only be made by a limited number of the Sky's staff. As at the date of this Agreement, Sky's staff who will have the ability to make telephone requests shall be:

- S.40(2) [redacted] (Investigations Manager),
- S.40(2) [redacted] (Investigator)

6.2.4. Sky may update this list by notice to ACRO from time to time.

7. Provision of Information

7.1. **Response to a PNC Names Enquiry Search / Witness Search**

7.1.1. In response to a formal written application, ACRO will provide a Disclosure Print to The Agency with the following information derived from the PNC in response to applications made in accordance with this Agreement:

- All convictions, cautions, warnings and reprimands.
- Additional information as deemed relevant by ACRO where there is a pressing social need to do so (via a Force Disclosure Unit as appropriate).

7.1.2. The exception to this is if a witness check is conducted then a 'Witness Print' will be provided.

7.1.3. As per clause 5.1.3 of this Agreement, a 'Prosecutors/Court Multiple PNC Print' will only be provided as part of the ASN creation process in relation to a current prosecution.

7.1.4. If Sky require an additional copy of the 'Prosecutor's and Court Multiple Print' or a 'Witness Print' then this should be made clear in the correspondence submitted by The Agency. Such requests will be charged in accordance with the letter of charges provided separately to Sky.

7.1.5. PNC Warning Signals will not be disclosed.

7.1.6. 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 Sky.

7.1.7. If Sky 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 S.31(1)

7.1.8. Sky will need to liaise directly with forces to obtain further explanation of specific information regarding the offending revealed in the prints provided under this Agreement or to gain access to statements, interviews under caution etc. relating to any previous offending. Forces may apply their own charges in respect of any information they disclose.

8. Recording Convictions on the PNC

8.1. **Creating Records on the PNC**

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

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

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

8.1.4. As part of the record creation service provided by ACRO, Sky will be sent a PNC Prosecutor's and Court Multiple 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. When a prosecution by Sky 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 Sky is to advise ACRO of any adjournments or disposal handed down by the court using the form which will be supplied by ACRO separately.

8.1.6. If, once a PNC record has been created by ACRO and an ASN issued to Sky, 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), Sky will inform ACRO as soon as reasonably practical in order that the PNC record can be updated.

9. International Requests

9.1. **Process**

9.1.1. S.31(1) [redacted]

S.31(1) [redacted]

9.1.2. The purpose of this process is to enable the subject's full criminal history to be made available to the relevant Judicial Authority e.g. the court at which the case is being heard. Sky shall act as representatives of the Judicial Authority in this process.

9.1.3. ACRO can submit requests to EU and non-EU countries for criminal conviction information. The process of this is detailed in clauses 9.2 and 9.3.

9.1.4. Transfers for general processing may rely on Adequacy or in Specific Circumstances where the transfer is necessary for important reasons of public interest, or when necessary for the establishment, exercise or defence of legal claims.

9.1.5. Requests should be made using the International Request form which will be supplied by ACRO separately; and sent, one request per e-mail, from the nominated Agency mailbox to the ACRO International Requests Mailbox: S.31(1) [redacted] Erroneous or incomplete forms may delay the processing of the request.

9.1.6. ACRO will receive requests from Sky, via the following secure mailbox: S.31(1) [redacted]

9.1.7. ACRO will forward the request to the relevant national authority/ies for a response as per the instances set out in clauses 9.2 and 9.3.

9.1.8. Requests may be rejected if there is insufficient information to enable the requested country to verify the identity of the subject, or if the mandatory nominal information is not supplied. Requests may not be sent if the requested country does not have a criminal register or is categorised as an extreme/severe risk country. Guidance on the required information will be sent to Sky separately, and ACRO will send updated copies if this information changes.

9.1.9. Once a response has been received from the country of nationality, ACRO shall forward the conviction/non-conviction information, including any necessary translation, to the nominated Sky mailbox utilising the email security platform KnowBe4 (formerly known as EGRESS).

9.2. **Exchange of Criminal Records with the EU**

9.2.1. If the subject is an EU national, then ACRO shall deal with the request under the 1959 Convention on Mutual Assistance in Criminal Matters and the EU-UK Trade Co-operation agreement between the European Union and the United Kingdom, Part 3, Title IX on the exchange of information extracted from the criminal record.

9.2.2. There is a mandated response time of 20 working days for the requested country to respond. This includes responses containing criminal convictions, responses specifying a subject is no trace or has no convictions in the requested country or a notification that the country cannot respond for the intended purpose of the check.

9.2.3. The Central Authority of each EU Member State shall reply to requests made for purposes other than that of criminal proceedings in accordance with their own domestic law. This means that a country may respond stating that they cannot disclose information depending on the purpose of the request.

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

9.2.5. Requests made outside of criminal proceedings may not be responded to, and are subject to legislation and processes in the requested country. Guidance on which countries may respond to requests outside of criminal proceedings can be provided to Sky by ACRO, however this does not guarantee that a response will be provided.

9.3. Exchange of Criminal Records with Non-EU Countries

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

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

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

9.4. Specific Data Handling

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

9.4.2. Any data obtained from the European Economic Area (EEA) cannot be onward transferred either by ACRO or Sky to a Third Country[1] without consent from the originator, except where the transfer is necessary for

[1] As defined in clause 2.1.1.

Specific Circumstances, in which case the originator will be notified after the fact.

10. Information Security

10.1. Government Security Classification Policy

10.1.1. 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.

10.1.2. 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.

10.2. Security Standards

10.2.1. 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.

10.2.2. 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.

10.2.3. 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.

10.2.4. 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.

10.2.5. 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.

10.3. **Volumes**

10.3.1. S.31(1) [redacted]

10.3.2. Sky will advise ACRO if the number of PNC Checks/International Requests/PNC Updates is likely to be exceeded.

10.3.3. 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.

10.4. **Transmission**

10.4.1. With the exception of telephone requests in cases of emergency, contact between ACRO and Sky should only be made over a secure communication network using the agreed S.31(1) [redacted] on the part of Sky and an equivalent secure method on the part of ACRO, and care must be taken where personal information is shared or discussed.

10.4.2. 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.

10.4.3. The Sky reference number must be included in the subject field of every e-mail sent to ACRO.

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

10.5. **Retention and disposal**

10.5.1. 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.

11. Information Management

11.1. Accuracy of Personal Data

11.1.1. 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.

11.1.2. Where a partner rectifies personal data, it must notify any Competent Authority from which the inaccurate personal data originated, and should notify any other Controller of the correction, unless a compelling reason for not doing so exists.

11.1.3. 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.

11.2. Accuracy Disputes

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

11.3. Turnaround

11.3.1. This Agreement requires a S.31(1) turnaround (not including day of receipt or response) on all requests submitted to ACRO for PNC data, except where ACRO requires further information from Sky to make a positive match. In these circumstances, ACRO will process the enquiry when the required information has been supplied by The Agency.

11.3.2. For turnaround times for International Requests please see clause 9 of this Agreement.

11.3.3. Responses to requests for additional information must be made by Sky within S.31(1) (not including day of receipt or response). If ACRO do not receive the information, the request will be closed.

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

11.3.5. An exception to the S.31(1) 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.

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

11.3.7. ACRO will complete/update a record on the PNC within S.31(1) (not including day of receipt or response) of the receipt of a completed NPA form from Sky in respect of every person for whom a PNC record is to be created.

11.4. **Quality Assurance and Control**

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

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

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

12. Complaints and Breaches

12.1. **Complaints**

12.1.1. 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 Controller will consult with other parties where appropriate.

12.2. **Breaches**

12.2.1. 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).

12.2.2. 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.

12.2.3. In the event of a dispute or claim brought by a data subject or the Supervisory Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will co-operate with a view to settling them amicably in a timely fashion.

12.2.4. 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.

12.2.5. All security incidents and breaches involving police data shared under this Agreement must be reported immediately to the single points of contact (SPOCs) designated in this Agreement.

13. Information Rights

13.1. **Freedom of Information Act 2000**

13.1.1. 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 Minister for the Cabinet Office's Code of Practice issued under section 45 of the FOIA and the Secretary of State's Code of Practice under Regulation 16 of the EIR.

13.1.2. 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.

13.1.3. 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 Sky 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

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

13.2. **Data Subject Information Rights**

13.2.1. 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.

13.2.2. 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.

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

13.2.4. Where Sky receives a relevant request, the Sky representative is to contact the ACRO Data Protection Officer at: S.31(1) [redacted] to ascertain whether ACRO wishes to propose to the Sky that they apply any relevant exemptions when responding to the applicant.

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

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

13.3. **Fair processing and privacy notices**

13.3.1. 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.

13.3.2. 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 The Agency 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.

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

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

14.1. 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.

15. Roles and responsibilities

15.1. **Single Point of Contact**

15.1.1. ACRO and The Agency 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
  S.31(1) [redacted]
  [redacted]
- ACRO (International requests):
  ACRO International Services Head of Section
  S.31(1) [redacted]
  [redacted]
  [redacted]
- Sky UK Limited:
  S.40(2) [redacted] Investigations Manager
  S.40(2) [redacted]
  [redacted]

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

15.1.3. 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.

15.2. **Escalation**

15.2.1. 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
  S.31(1) [redacted]
  [redacted]
- ACRO (International requests):
  ACRO International Services Deputy Manager
  S.31(1) [redacted]
  [redacted]
  [redacted]
- ACRO (Information Sharing Agreement):
  ACRO Information Governance Team
  S.31(1) [redacted]
  [redacted]
- Sky UK Limited:
  S.40(2) [redacted]
  Group Head of intelligence and investigations
  S.40(2) [redacted]
  [redacted]
- Sky UK Limited:
  SKY data protection officer
  dp.department@sky.uk

15.2.2. Both ACRO and Sky 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.

16. Charges

16.1. **Price and Rates**

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

16.2. **Invoices**

16.2.1. 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 The Agency).

16.2.2. The Purchase Order Number is to be provided by Sky 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.

16.2.3. Sky 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 Sky.

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

17. Review

17.1. **Frequency**

17.1.1. This Agreement will be reviewed annually.

17.1.2. Renewal of this Agreement will be considered annually.

17.1.3. This Agreement will run for 12 months from the "Date Issued" as per the Summary Sheet on Page 2. The date issued will be determined by the date of the last signatory to this Agreement.

18. Variation

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

19. Waiver

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

20. Severance

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

20.2. If any provision or part-provision of this Agreement is deemed deleted under clause 20.1, the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

21. Changes to the applicable law

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

22. No partnership or agency

22.1. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, make any party the agent of the other party, or authorise any party to make or enter into any commitments for or on behalf of any other party. Each party confirms it is acting on its own behalf and not for the benefit of any other person.

23. Notice

23.1. 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.

23.2. 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.

23.3. 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.

23.4. 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.

23.4.1. 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.

23.5. 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.

24. Signature

24.1. Undertaking

24.1.1. 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.

24.1.2. Signatories must ensure compliance with all relevant legislation.

Signed on behalf of ACRO Senior Information Risk Owner (SIRO)	Signed on behalf of Sky UK Limited
Signature: S.40(2) [redacted]	Signature: Using Adobe- Docu Sign Signed by: S.40(2) [redacted]
Full Name: Julian Fletcher	Full Name: S.40(2) [redacted]
Position Held: CEO of ACRO	Position Held: Group Head of AP I&I
Date: 22nd October 2025	Date: 22 October 2025

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

Signed as NPCC Lead Controller for PNC/LEDS	
S.40(2) [redacted]	Full Name: Nav Malik
	Position Held: Deputy Chief Constable, National Police Chiefs' Council Law Enforcement Data Service (NPCC LEDS)
	Date: 23/10/2025